



**HAL**  
open science

# Géométrie discrète, calcul en nombres entiers et algorithmique

Jean-Pierre Reveillès

► **To cite this version:**

Jean-Pierre Reveillès. Géométrie discrète, calcul en nombres entiers et algorithmique. Traitement des images [eess.IV]. Université Louis Pasteur, 1991. <tel-01279525>

**HAL Id: tel-01279525**

**<https://hal.science/tel-01279525v1>**

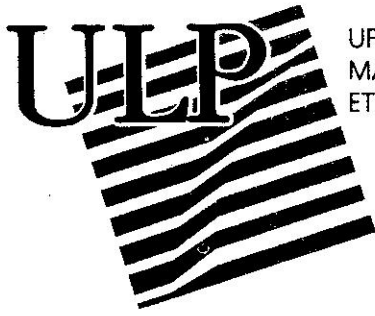
Submitted on 28 Feb 2016

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization



UFR DE  
MATHÉMATIQUE  
ET D'INFORMATIQUE

Thèse d'Etat

GEOMETRIE DISCRETE, CALCUL EN NOMBRES ENTIERS  
ET  
ALGORITHMIQUE.

par J.P. REVEILLES

JURY :

J.P. RAMIS : Président  
P. CARTIER : Rapporteur  
J. BERSTEL : Rapporteur  
J.M. CHASSERY : Examineur  
J. FRANCON : Directeur

Soutenu le 20-12-91.

## REMERCIEMENTS

Ce travail doit beaucoup aux critiques, encouragements, discussions, souvent longues et animées, aux invitations à en exposer des parties, que de nombreux collègues mathématiciens et informaticiens m'ont accordés. A tous et surtout, ceux qui le connaissent savent qu'un mot suffit, à G. Reeb: merci.

## CONTENU

Les numérisations variées conduisent souvent à des cohabitations difficiles sinon des conflits entre discret et continu. Les analyses de nombreuses situations de ce type montrent la plupart du temps que l'origine des problèmes réside dans l'emploi simultané de nombres réels et de nombres entiers, aux propriétés bien distinctes.

Contrairement à l'approche traditionnelle de ces questions, qui traite "individuellement", objet par objet, les relations discret-continu, nous adoptons un point de vue "global", pour une théorie complète. Nous proposons dans la première partie une solution possible de ces conflits par l'usage de Théories où les nombres réels sont remplacés par des entiers; les notions continues (ou topologiques) sont retrouvées simplement en utilisant la notion d'entier infiniment grand de l'Analyse Non Standard. Bien qu'un très grand nombre de domaines, tant en Mathématique qu'en Physique, soient concernés il nous a semblé clair que l'Informatique, autre source de problèmes discret-continu importants, pouvait offrir un champ d'expérimentation à ces idées.

Nous donnons en particulier les fondements d'une Géométrie Discrète Arithmétique, pendant discret de la Géométrie Euclidienne; elle occupe la deuxième partie. C'est une mathématisation immédiate de la pratique du discret-continu géométrique, domaine qui va de l'Algorithmique Graphique à la Conception des Circuits en passant par la Géométrie Algorithmique, la Synthèse d'Images etc.; elle permet de résoudre de nombreuses questions concrètes posées dans ces domaines. L'émergence de cette théorie est certainement le résultat le plus significatif de ce travail. Nous nous contentons dans ce descriptif de mentionner quelques résultats pouvant donner une idée de l'intérêt de cette Géométrie.

Nous donnons une définition des droites discrètes qui contient les notions antérieures les plus courantes, s'accompagne d'une riche collection de théorèmes de structures pour concevoir des algorithmes. Malgré l'arithmétisation qui intervient dans cette définition l'algorithmique qui s'en déduit n'est pas pénalisée, bien au contraire.

Nous avons également mis la structure des droites discrètes en correspondance avec celle du groupe modulaire ce qui présente les avantages suivants:

- o interprétation géométrique de chaque paramètre de la définition précédente et de l'action des transformations planes sur les droites discrètes;

o mise en évidence d'un accord entre la description abstraite des transformations géométriques et l'architecture des machines, les transvections correspondant à des transformations de blocs-mémoires;

o jonction entre la Géométrie Discrète et l'Analyse Matricielle en nombres entiers, ce qui garantit une généralisation aisée dans les dimensions supérieures.

Aucune des définitions antérieures de la littérature ne définit des objets intrinsèques; mais elles donnent des algorithmes de tracé, ou des processus d'identification efficaces. Une grande partie de notre travail consiste à montrer que la notion intrinsèque introduite ne pénalise pas l'algorithmique existante; elle permet même de faire mieux. Nous présentons une douzaine d'algorithmes, pour la plupart nouveaux, de parcours (point par point) ou de tracé (par blocs) itératifs ou récursifs, de ces objets. Certains sont obtenus assez facilement à l'aide du calcul modulaire. D'autres, les plus performants, nécessitent de dégager quelques théorèmes de structure. Le meilleur d'entre eux (deuxième partie, première section, §V 4) ramène le tracé d'une droite 8-connexe de pente rationnelle  $\frac{a}{b}$  à environ  $\log(a)$  opérations de translations sur des blocs mémoire. Un autre, dit de clivage, (deuxième partie, première section, §VII 4) permet de supprimer certaines étapes de l'algorithme d'Euclide.

Pour obtenir un algorithme récursif le plus souple possible et également pour étudier la décomposition d'un segment discret en sous-segments nous abordons l'étude des relations entre les décompositions homographiques des rationnels et la structure des droites discrètes dont ils sont les pentes: clivage des rationnels et théorème du mélange qui permet de reconstituer la structure d'une droite de pente  $\frac{am+a'm'}{bm+b'm'}$ , en fonction de celles associées aux pentes  $\frac{a}{b}$ ,  $\frac{a'}{b'}$ , et  $\frac{m}{m+m'}$ , (deuxième partie, première section, §VII 1).

Ainsi armé il n'est alors pas trop difficile d'apporter la réponse au problème de l'intersection de deux droites discrètes (aucun algorithme, sinon le balayage évident, n'existe dans la littérature); cette réponse montrant que le parcours d'une intersection restant de même complexité que celui d'une droite unique (deuxième partie, deuxième section, §III 2). Mais, toujours à cause de la définition de droite admise en Géométrie Discrète, l'intersection joue un rôle beaucoup plus important qu'en Géométrie Euclidienne. Il est important de dégager ses spécificités fort nombreuses: les divers cas d'intersection, le nombre de points de l'intersection, la connexité..., qui forment un chapitre de notre travail.

Ces premiers pas concernant l'étude des droites discrètes nous ont fait découvrir quelques résultats inattendus: l'enveloppe convexe des points d'un

réseau entier, le pavage simultané de deux droites et les transformations entre intersections (relation avec le groupe modulaire deuxième partie, deuxième section, §IV).

Nous en avons également déduit un moyen d'exprimer par une formule rigoureuse le nombre de points d'un réseau entier contenus dans un rectangle isothétique (deuxième partie, première section, §VIII) et un moyen de résoudre les inégalités modulaires, i.e. les inéquations du type

$$(a.x \text{ mod } b) \leq h$$

a, b, h entiers donnés (cf deuxième partie, première section, §V 3).

Nous avons regroupé dans la troisième section de cette deuxième partie les applications de la Géométrie Discrètes à l'un des problèmes importants du traitement des images: celui des propriétés métriques des transformations géométriques. Le problème de la rotation, que nous évoquons dans la première partie, est parmi les plus typiques. Nous l'abordons par deux voies indépendantes qui utilisent des notions de droites discrètes un peu plus générales que la précédente. Nous obtenons deux algorithmes: la rotation compensée (§ II de cette section) et la rotation-permutation (§ III) qui détermine, pour tout réel  $\alpha$ , une permutation de  $\mathbb{Z}^2$  très voisine de la rotation réelle d'angle  $\alpha$ . Comme cette rotation-permutation se comporte numériquement comme la rotation réelle tronquée on devine immédiatement son intérêt.

Nous testons les qualités et défauts de ces rotations discrètes à travers une simulation discrète du phénomène de Moiré (§ V de cette 3<sup>e</sup> section) qui regroupe par ailleurs d'autres aspects de la Géométrie Discrète.

De façon analogue, l'Analyse remplaçant la Géométrie, nous apportons dans la troisième partie une méthode, le Calcul en Nombres Entiers, de conception d'algorithmes efficaces, "en nombres entiers". Cette partie s'appuie sur les bases infiniment grandes introduites dans la première partie. Elle s'attache, comme la précédente, à montrer que cette notion "abstraite" a aussi des implications concrètes utilisables pour les machines classiques. En particulier elle nous conduit à revoir la question de la gestion des retenues dans les arithmétiques fixes ou flottantes ce qui nous donne une classe très générale d'algorithmes rapides permettant de parcourir les ensembles de points entiers par défaut des fonctions usuelles de l'Analyse: polynômes, fonctions trigonométriques, solutions d'équations différentielles, ensembles fractals.

## TABLE DES MATIERES.

Première partie

### LES THEORIES DISCRETES IDEALES.

#### INTRODUCTION

- I LES CONFLITS DISCRET-CONTINU ET LA THESE CLASSIQUE.
  - 1 L'approximation numérique.
  - 2 La discrétisation en Géométrie et les conflits qu'elle provoque.
  - 3 La thèse classique.
  - 4 Comment réconcilier le Discret et le Continu ?
  
- II UNE NOUVELLE APPROCHE DES RELATIONS DISCRET-CONTINU.
  - 1 Atomisme et ordres de grandeur.
  - 2 Le modèle finitaire et le Discret Idéal.
  - 3 L'hyperordinateur.
  - 4 Le contenu des théories discrètes idéales.
  
- III UTILISATION PRATIQUE DE LA NOUVELLE APPROCHE DISCRET-CONTINU.
  - 1 La chaîne d'hyperordinateurs.
  - 2 Les avantages des objets paramétrés.
  - 3 Les relations entre les Théories Discrètes et les Théories Discrètes Idéales.
  - 4 Applications algorithmiques de l'hyperordinateur: Le Calcul en Nombres Entiers.
  - 5 L'émergence d'une théorie: la Géométrie Discrète.
  - 6 La coexistence avec d'autres théories discrètes.

Deuxième partie  
LA GEOMETRIE DISCRETE.

INTRODUCTION

Première section  
LES DROITES DISCRETES.

I UNE NOTION GENERALE DE DROITE DISCRETE.

- 1 La position du problème.
- 2 Définition diophantienne des droites discrètes.
- 3 Droites discrètes équivalentes.
- 4 Le rôle du reste d'une droite discrète. Le calcul modulaire.
- 5 La topologie des droites discrètes.
- 6 Relation avec les notions antérieures.
- 6 Symétries des droites discrètes.

II DROITES DISCRETES ET GROUPE  $Sl(2, \mathbb{Z})$ .

- 1 Droites discrètes homologues.
- 2 Paliers et groupe modulaire.

III LES PREMIERS ALGORITHMES DE TRACE.

- 1 Le tracé des droites naïves.
- 2 Parcours et tracés des droites \*-connexes.
- 3 Le tracé des droites généralisées: algorithme des vecteurs pilotés.
- 4 Le tracé des droites épaisses.

IV LES PROPRIETES MODULAIRES DES DROITES DISCRETES.

- 1 Le mot de Christoffel et le mot de paliers d'un rationnel.
- 2 L'algorithme de Christoffel.
- 3 Les séquences montantes de la suite des restes et les paliers des droites discrètes.
- 4 L'algorithme de tracé par paliers.
- 5 La structure du mot de paliers.

V LES BASES EUCLIDIENNES D'UN RESEAU ET LEURS APPLICATIONS.

- 1 L'algorithme de Jacobi-Perron et les bases euclidiennes d'un réseau entier.
- 2 Une généralisation du diagramme de Klein aux réseaux entiers.
- 3 Quelques inégalités modulaires.
- 4 Les bases euclidiennes et les droites discrètes; nouveau tracé.

- 5 Le parcours des points d'un réseau dans un rectangle isothétique.
- 6 Le paramétrage des points d'un réseau dans une fenêtre euclidienne.
- 7 La résolution des inéquations modulaires.

#### VI LES MINIMA DU RESEAU DES RESTES.

- 1 Enveloppe convexe et continuants de Fantet de Lagny.
- 2 Les vecteurs minimaux du réseau des restes.
- 3 Les continuants et les fins de paliers des droites discrètes.

#### VII LE CLIVAGE D'UN RATIONNEL.

- 1 Le théorème du mélange des mots de paliers.
- 2 Une suite de rationnels liée aux paliers des droites discrètes.
- 3 Le dévissage et la reconstruction d'un mot de paliers.
- 4 Algorithmes de construction d'un mot de paliers; nouveaux tracés.
- 5 Les droites discrètes et les mots de Sturm.

#### VIII LE DENOMBREMENT DES POINTS D'UN RESEAU ENTIER DANS UNE FENETRE ISOTHETIQUE ET LE "Lattice problem".

- 1 Le calcul d'une intégrale associée à une droite discrète.
- 2 Les points d'un réseau dans un rectangle isothétique.
- 3 Droites discrètes et résidus quadratiques.

### Deuxième section

#### L'INTERSECTION DES DROITES DISCRETES

#### I INTERSECTIONS ENTIERES ET INTERSECTIONS RATIONNELLES.

#### II QUELQUES CAS PARTICULIERS.

- 1 Le cas des numérateurs consécutifs.
- 2 Les numérateurs quelconques et les épaisseurs déterminantales.

#### III DROITES DISCRETES ET RESEAUX ENTIERS.

- 1 Un réseau pour deux droites.
- 2 Paramétrage de l'intersection de deux droites.

#### IV INTERSECTION ET GROUPE $S_1(2, \mathbb{Z})$ .

#### V CONNEXITE DE L'INTERSECTION.

Troisième section  
ROTATIONS DISCRETES ET APPLICATIONS.

- I LES APPROCHES EXISTANTES DE LA ROTATION DISCRETE.
- 1 La rotation réelle tronquée.
  - 2 La rotation par droites discrètes.
- II LA ROTATION COMPENSEE.
- 1 Les droites compensées et l'invariance par rotation.
  - 2 Le balayage par les droites compensées et la rotation discrète.
  - 3 Les défauts de la rotation compensée.
- III AUTRES TRANSFORMATIONS.
- IV LE MOIRE ARITHMETIQUE.
- Introduction
- 1 Les lois générales du Moiré.
  - 2 Les équations des franges.
  - 3 Le théorème de convolution de Harthong.
  - 4 Le Moiré de droites euclidiennes.
  - 5 La discrétisation du Moiré.
  - 6 Les lois du Moiré arithmétique.
  - 7 Le problème des grilles isométriques.

Troisième partie:  
LE CALCUL EN NOMBRES ENTIERS.

INTRODUCTION

- I LA GESTION DES RETENUES ET LA CONVERSION DES ALGORITHMES.
- 1 Les entiers en base  $\omega$  et la gestion des retenues.
  - 2 La conversion d'une formule.
  - 3 Expression d'une somme en base  $\omega$ .
  - 4 Calcul des monômes en base  $\omega$ .
  - 5 Le produit  $a \left(1 + \frac{X}{\omega}\right)^n$  et l'exponentielle arithmétique.
  - 6 Les monômes  $\left[ \frac{a_0 a_1 \dots a_n}{\omega^n} \right]$ .

## II POLYNOMES EN NOMBRES ENTIERS

- 1 Les formules différentielles.
- 2 Evaluation des polynômes réels: Taylor en Nombres Entiers.
- 3 Les algorithmes approchés.
- 4 L'algorithme d'évaluation d'ordre 1 des polynômes.
- 5 Evaluation par la formule de Horner.

## III EQUATIONS DIFFERENTIELLES EN NOMBRES ENTIERS.

- 1 Intégration numérique de l'équation  $y'=y$  en nombres entiers.
- 2 Evaluation rapide de la fonction exponentielle.
- 3 Implémentation de l'algorithme 1 en langage machine.
- 4 L'algorithme d'Euler modifié en nombres entiers.
- 5 Implémentation de l'algorithme 2 en langage machine.
- 6 Logarithme et nombres entiers.
- 7 La fonction  $\sqrt{x}$  en nombres entiers.
- 8 Coniques.
- 9 Cercles discrets.
- 10 L'équation du pendule forcé.

## IV CALCUL EN NOMBRES ENTIERS ET ALGORITHMES RAPIDES POUR L'ENSEMBLE DE MANDELBROT.

- 1 Le premier algorithme rapide: une famille de systèmes dynamiques quadratiques sur  $\mathbb{Z}^2$ .
- 2 Résultats pratiques.
- 3 Un algorithme exploitant la dynamique.
- 4 L'algorithme dichotomique.

Première partie

LES THEORIES DISCRETES IDEALES.

## INTRODUCTION

Dans cette première partie nous allons, de la simple existence d'entiers infiniment grands, tels qu'ils sont présentés dans I.S.T. (cf [74]), tirer quelques conséquences de portée générale sur certaines machines infiniment puissantes, leurs possibilités et ce qu'elles apportent aux utilisateurs des machines ordinaires.

Une grande part des difficultés rencontrées dans l'étude du monde réel provient du fait que l'outil théorique avec lequel nous le décrivons ne reproduit pas bien la teneur de son dosage entre le discret et continu. Or notre arsenal d'outils s'est enrichi aujourd'hui de machines concrètes, finies, plus nettement marquées de l'empreinte du monde physique que nos modèles formels, peut-être trop fascinés par le continu. Il est compréhensible d'une part qu'un hiatus apparaisse entre les deux outils, numérique et théorique, et d'autre part que ces machines, nous obligeant à mieux coller à la réalité, participent aussi à l'effort de compréhension de sa composition et de ses structures cachées.

Les avancées récentes des disciplines concernées par le fini et le numérique: Informatique, Mathématiques Appliquées, certains domaines de la Physique et de la Technologie, montrent que l'interprétation du monde réel en termes discrets est certainement accessible mais difficile. La question du contenu effectif, du possible et des limites des Mathématiques Discrètes est aujourd'hui un sujet essentiel.

La description admise de la Nature (même aperçue au travers d'un écran d'ordinateur ou d'un microscope) requiert déjà un grand nombre d'outils: nombres naturels, groupes, combinatoire, théorie des langages, automates, etc. Pourtant ceux-ci ne suffisent pas: elle en réclame constamment d'autres qui, paradoxalement, sont d'inspiration continue. Expliquons-nous. L'usage d'entités technologiques exclusivement finies et discrètes, processeurs, pixels, voxels ou la rencontre, dans l'infiniment petit, des structures atomiques obligent ces Sciences à ériger des répliques discrètes de l'Analyse, de la Topologie et de la Géométrie, voir de chapitres de la Physique: Mécanique, Acoustique, Optique. Le constat, renouvelé dans ces domaines, de la difficulté de la Mathématique Discrète conduit à la recherche d'analogues discrets des objets et théories continus existant dans la discipline classique correspondante. C'est, pour les spécialistes de la description de la Nature, l'espoir de comprendre le discret-complicé à partir du continu-simple.

Cette recherche parallèle, placée sur un sol plus accidenté, ne peut pas, malgré les analogies du relief, copier exactement le comportement suivi en face sur une terre idéale; elle tente malgré tout de s'en inspirer. Il serait certainement avantageux et bénéfique pour tous d'harmoniser la description de ces deux territoires, trop souvent considérés comme irrémédiablement éloignés, en construisant des théories mathématiques simultanément discrètes et continues, à la fois voisines des théories idéales et déformables en outils directement utilisables dans le monde discret. C'est, sous une forme à peine nouvelle, le vieux thème du rapport entre le discret et le continu.

Nous savons depuis longtemps que le désaccord entre le Discret et le Continu se mesure par un éloignement "infini" pris en compte dans l'un des axiomes fondateurs de la Mathématique. Le concept de nombre entier infiniment grand, nous permet d'envisager une Mathématique Discrète Idéale intermédiaire entre la classique Mathématique du Continu et la Mathématique Discrète; comme la pile d'un pont entre deux rives. Nous pouvons même envisager une "infinité" de telles Mathématiques, formant une famille de théories très proches les unes des autres, reliant le Discret au continu par une passerelle théorique. Cette chaîne de Théories Discrètes apporte un regard neuf sur les relations entre Discret et Continu. Le but de ce travail est de la construire et de l'utiliser. L'emploi que nous en ferons restera bien modeste au regard de la quantité d'applications qu'il faudrait examiner pour la confirmer ou l'infirmer avec certitude; souhaitons néanmoins que ces théories discrètes idéales potentielles puissent être perçues comme un encouragement à l'audace par tous les chercheurs engagés sur la voie de la description discrète des phénomènes continus.

## I LES CONFLITS DISCRET-CONTINU ET LA THESE CLASSIQUE

Les ordinateurs sont des machines discrètes: tout traitement informatique ne peut manipuler qu'un nombre fini de symboles, même si ce nombre est très grand au regard d'un calculateur humain. Il en est d'ailleurs de même d'un calculateur humain. Ces outils ne peuvent donc pas utiliser immédiatement la modélisation de la Nature construite à partir du continu. Ce hiatus est la source de conflits que nous regrouperons en deux classes. La première concerne les questions d'approximation numérique, la seconde les problèmes de discrétisation de propriétés plus générales, par exemple géométriques ou topologiques.

### 1 L'approximation numérique

Les données géométriques, points, droites, segments, cercles,... du monde euclidien continu, sont, en général, représentées dans les calculs théoriques

via des nombres réels; mais dans les calculs pratiques, en machine ou à la main, ils sont réduits, en dernière instance, à des calculs sur une famille finie de nombres entiers. On peut, certes, effectuer des calculs "formels", par exemple traiter les nombres  $\pi$  et  $\sqrt{2}$  comme des symboles accompagnés de règles de calcul particulières, comme  $\sqrt{2}^2$  se réécrit 2; mais ceci alourdit les traitements et ne peut pas être employé constamment.

Du point de vue du calcul effectif, les nombres réels sont idéaux, (dans le sens qu'ils font appel à l'**axiome de l'infini** déjà dans leur définition et portent en général une quantité d'information infinie), seuls les entiers (et les objets dérivés par des procédés finitaires) peuvent avoir une réalité en termes de bits dans une machine ou de chiffres sur une feuille de papier, ou en termes de points sur un écran ou produits par une imprimante ou un traceur digital. Les représentations couramment utilisées (virgule fixe, virgule flottante) pour les calculs numériques sont en général approchées et les calculs produisent des erreurs dites d'arrondi; les opérations effectives sur ces représentations ne sont en général ni associatives, ni distributives,...; elles ne vérifient pas les axiomes du corps des nombres réels. Ces questions sont bien connues et forment tout un chapitre de l'analyse numérique, chapitre appelé analyse d'erreur (cf par exemple [119]), particulièrement étudié pour les calculs algébriques classiques comme l'algèbre linéaire, avec des résultats étonnants. Toutefois cette approximation numérique ne s'applique bien qu'aux problèmes effectivement décrits par des fonctions numériques.

## 2 La discrétisation en Géométrie et les conflits qu'elle provoque.

Dans les calculs algébriques ou géométriques les erreurs d'arrondi produisent des résultats erronés; mais dans les derniers des effets parasites plus subtils apparaissent aussi: certains algorithmes ne terminent pas. Ce phénomène, du à la naissance des cycles qui accompagnent la composition d'un processus itératif convergent avec une application de troncature, révèle en général que l'on a appliqué un algorithme utilisant des constructions de Géométrie Euclidienne à des données discrètes. De façon générale dès que des données ont été tronquées plus aucun théorème géométrique n'est vrai. On peut dire alors que la géométrie, qui, sur le papier, était déjà l'art de raisonner juste sur des figures fausses, devient, sur machine, l'art de raisonner juste à partir de calculs faux produisant des figures fausses, si toutefois les calculs terminent. Donnons quelques exemples d'effets pervers de la troncature qui détruit les propriétés des objets de la Géométrie Euclidienne.

a) Les droites

La situation suivante n'est pas rare en Conception Assistée par Ordinateur. On affiche un segment de droite réelle d'extrémités A et B sur un écran, par la méthode dite de Bresenham (cf [10]); il en résulte un ensemble de pixels comme sur la figure 1; les gros points sont ceux du segment, P est le discrétisé de A et Q celui de B. Un opérateur désigne alors un pixel R du segment discret (à l'aide d'un dispositif d'entrée interactive comme une souris). Il commande ensuite un effacement du segment RQ.

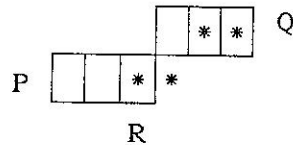


Figure 1

Sur la figure précédente les pixels du segment de Bresenham RQ sont indiqués par les "\*". Un point du segment discret PQ est oublié et tandis qu'un point de RQ n'appartient pas à PQ. L'effacement d'un sous-segment d'un segment discret produit en général des résultats incorrects. Ce phénomène indésirable vient de ce que la méthode de Bresenham "oublie" les points A et B du plan euclidien pour calculer les pixels des segments discrétisés PQ et RQ. Une autre méthode de discrétisation peut être définie et éviter ce phénomène, à condition qu'aucune erreur d'arrondi n'intervienne dans les calculs, ce qu'on ne sait pas vraiment contrôler.

b) Les transformations planes

Considérons le problème des plus concrets suivant (qu'on rencontre, par exemple, en "publication ou édition assistée par ordinateur"): on dispose d'une image digitalisée sous forme d'un pictogramme et on veut effectuer sur ordinateur une rotation de ce pictogramme (par exemple pour imprimer le résultat parmi d'autres images ou du texte sur une page). Les calculs à effectuer sont bien connus (même de certains lycéens): aux coordonnées  $x$  et  $y$  (supposées ici entières) de chaque pixel de l'image il suffit d'appliquer une transformation linéaire (où  $\alpha$  est l'angle de rotation, le centre de rotation étant supposé placé à l'origine du repère)

$$\begin{cases} x' = x \cos\alpha + y \sin\alpha \\ y' = -x \sin\alpha + y \cos\alpha \end{cases}$$

pour obtenir les coordonnées  $x'$  et  $y'$  d'un point; puis on approxime ce point par le point de coordonnées entières le plus proche et on affecte à ce point, qui est un pixel, la couleur du pixel de départ. On a donc traité les pixels

de l'image comme des points du plan euclidien usuel, on leur a appliqué une rotation dans cet espace et on a digitalisé le résultat pour l'afficher. Appelons ce procédé "rotation discrétisée". Il présente un inconvénient majeur. Dans cette transformation il y a perte d'information; très exactement cette transformation n'est pas une bijection de l'ensemble des points de coordonnées entières (pixels) sur lui même, alors que la rotation est une bijection du plan sur lui même. Pour s'en convaincre il suffit de prendre  $\alpha$  proche de  $\frac{\pi}{4}$  et les pixels de coordonnées (4,0) et (5,0); la rotation discrétisée fournit le même pixel pour les deux. La question de la couleur de ce même pixel se pose alors quand les pixels de départ sont de couleurs différentes. En pratique ce phénomène de perte d'information est suffisamment fréquent pour que la perte de qualité de l'image rotée puisse être sensible et l'édition de qualité ne peut s'en contenter. On ne connaît aujourd'hui aucune théorie qui fournisse une réponse convenable à l'édition de qualité, ni aucun procédé satisfaisant pour tourner la difficulté (d'après une note confidentielle d'un industriel américain, ce qui en passant, indique l'enjeu industriel de cette question). Il faut donc une géométrie discrète contenant une rotation aussi voisine que possible de la rotation euclidienne. Le fond de l'affaire est que les théorèmes de la géométrie euclidienne ne sont pas transportés par discrétisation. On trouvera une approche discrète de ce problème dans la deuxième partie.

### c) L'intersection de droites

L'usage de l'intersection de droites est très répandu; mais tout traitement numérique sur machine introduit, **de facto**, une discrétisation; or les droites discrétisées ne possèdent pas du tout les propriétés des droites usuelles vis à vis de l'intersection. La figure 2 suivante donne un exemple d'intersection de deux droites discrètes, la discrétisation étant induite par la structure régulière d'un écran. Celle qui est "cachée" derrière l'arithmétique flottante donnerait des droites nettement plus irrégulières ce qui accroîtrait notablement le problème de leur intersection. De plus cette dernière dépend du compilateur ou de la machine utilisé. Quant à tenir compte des deux discrétisations, ce qu'il faudrait faire en toute rigueur, nous n'y pensons même pas.

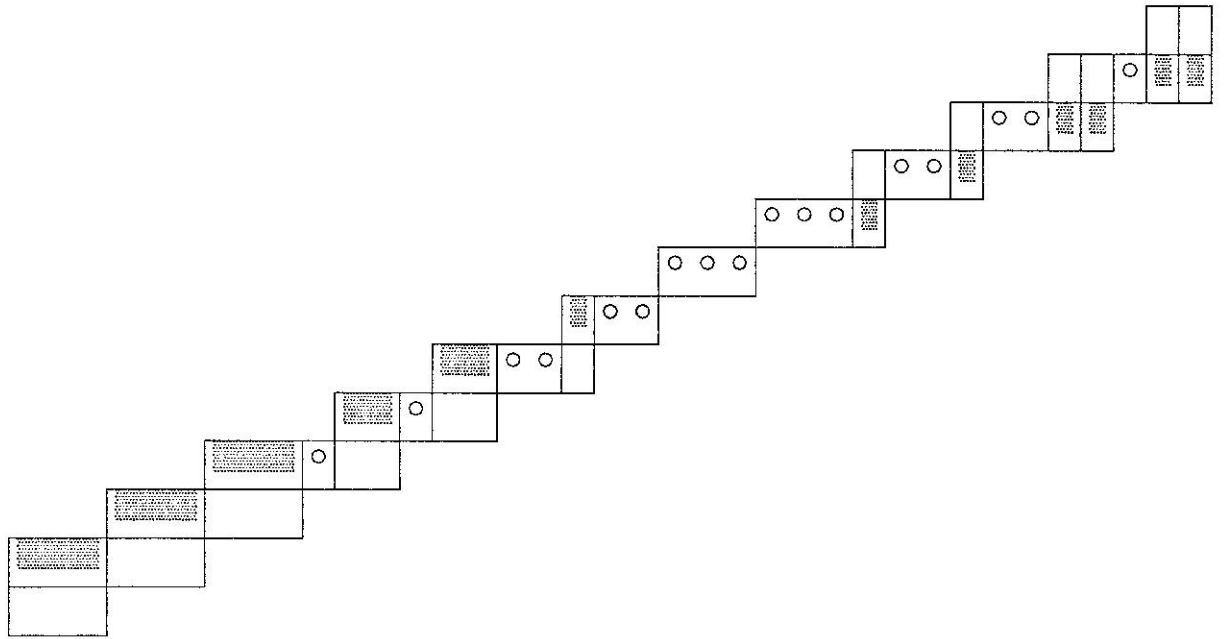


fig. 2

La composition de la Géométrie Euclidienne et de la troncature fait apparaître des versions discrètes des objets auxquels nous sommes habitués; mais ceux-ci ne réagissent plus du tout comme leurs originaux. Et, si l'on commence d'organiser ce territoire, des conflits internes apparaissent inévitablement dès qu'on l'étend tant soit peu. Si, par exemple, on est satisfait d'une notion de cercle discret, on pourra découvrir que ceux-ci ne feuilletent pas le plan: des trous apparaissent, ce qui peut être gênant dans certaines applications. Ce type de conflit interne est permanent et peut faire douter de l'existence, en théorie organisée, d'une Géométrie Discrète. La deuxième source de difficultés pour édifier des théories discrètes provient du bon choix des notions de base. Il n'existe plus, en général, de définition canonique des objets souhaités (droites, plans, cercles, courbes surfaces...) mais une multitude de possibilités qu'il est impossible d'étudier tour à tour et qui, de toute façon provoqueraient très vraisemblablement des conflits internes. La délimitation du territoire de la Géométrie Discrète est très difficile; pour les spécialistes actuels de cette discipline le problème essentiel se résume ainsi: quels sont les bons objets géométriques discrets ? Quelles sont leurs propriétés ?

C'est pour essayer de comprendre cette situation et d'apporter une réponse que nous introduisons les Théories Discrètes Idéales dans lesquelles les conflits internes et les questions de choix de définitions s'évanouissent. La considération du cas particulier de la Géométrie Discrète Idéale nous permet d'apporter quelques éléments de réponse à l'édification de la Géométrie Discrète. Nous exploitons même, dans la deuxième partie, ces

éléments de réponse dans le but de vérifier leur solidité et leur généralité.

d) La topologie discrète

La description algorithmique d'ensembles discrets (de pixels, de voxels) réclame parfois des généralisations des notions classiques tournant autour de la connexité. La géométrie ou la topologie des espaces euclidiens ne nous apportent aucune aide. Il faut construire une géométrie et une topologie discrètes dans lesquelles les notions de connexité, connexité simple,... ont un sens. L'étude de ces questions a été entreprise depuis fort longtemps par A. Rosenfeld (cf.[97], [98]) et continuée par de nombreux auteurs (cf. [62],[64],[67],[20],[21], [33],[77]). Grâce à eux l'essentiel a été retrouvé: ensembles connexes, trous, notions de courbe ou de surface discrète et on leur a étendu les théorèmes classique comme celui de Jordan pour en déduire des algorithmes divers. Malgré toute cette activité la tâche est loin d'être achevée (cf [101]) car les aspects métriques-discrets de ces questions y superposent des problèmes analogues à ceux que nous avons évoqués en a), b), c) et les rendent encore plus délicats.

### 3 La thèse classique

Pourtant la Géométrie Algorithmique, le Traitement de L'Image, la Synthèse d'Image ont pris leur essor dans les deux dernières décennies avec l'ambition d'être des outils effectifs utilisables dans les ordinateurs. La thèse aujourd'hui largement dominante dans ces disciplines est qu'on pense dans la géométrie usuelle fondée sur la notion de nombre réel et qu'on calcule avec des moyens techniquement imparfaits car limités; il s'ensuit que la "digitalisation" est vue comme un procédé d'approximation, avec perte d'information, comme l'échantillonnage d'un signal continu. La pensée est pure alors que les calculs sont impurs.

En conséquence, des corps de théorie et des procédés opératoires de calculs, de vérification et contrôle des erreurs sont mis en oeuvre par ceux qui appliquent la mathématique pour, en fin de compte et en principe, combler le fossé entre l'idéal mathématique et le techniquement faisable; en quelque sorte pour maîtriser l'imperfection technique.

Cette thèse et ces procédés pouvaient fonctionner tant qu'on arrivait à estimer une borne d'erreur sur le résultat d'un calcul. Mais quand les calculs ne terminent pas (en supposant qu'en pratique on arrive à pouvoir dire qu'un calcul ne termine pas) ou quand les propriétés idéales sur lesquelles est fondé l'algorithme ne se discrétisent pas bien ou quand interviennent deux discrétisations (le calcul et l'écran) la seule solution consiste à mémoriser des quantités énormes d'information conduisant à des traitements longs et

couteux.

#### 4 Comment réconcilier le Discret et le Continu ?

En reprenant les problèmes évoqués au §2 il serait souhaitable de pouvoir effacer un sous-segment d'un segment discret, faire tourner une partie d'une image discrète ou, de façon générale, effectuer des opérations de la géométrie euclidienne classique sur des objets discrets obtenus, directement ou pas, à partir d'objets continus. Nous venons de voir les problèmes posés si nous plongeons d'abord ces objets discrets dans un espace euclidien, puis leur appliquons des opérations définies dans cet espace, pour les rediscrétiser à nouveau. Ce traitement qui est le seul en vigueur est même plus compliqué dans d'autres cas comme l'effacement d'un sous-segment ou l'intersection de droites. Ce faisant on perd les propriétés et les théorèmes de la géométrie euclidienne usuelle alors qu'on voulait les garder. Les calculs terminent mais les résultats sont erronés. Finalement tous ces problèmes sont dus à l'absence de procédés de contrôle de la perte de propriétés après une troncature ou, ce qui revient au même, de la méconnaissance des propriétés des discrétisés des objets géométriques.

Dégageons ce qui se cache derrière ces souhaits. Ceci nous amènera à décrire les outils théoriques nécessaires pour les réaliser. Le coeur de l'affaire, à notre avis, consiste à pouvoir accéder à toute l'information contenue dans les diverses discrétisations d'un objet continu donné. Ceci implique que la donnée de l'objet implique la connaissance de toutes ses discrétisations; ou encore que l'objet contienne ses discrétisations. Ce désir peut se résumer ainsi: il faut construire le continu à partir du discret, progressivement et en suivant les lois de ce dernier.

Si nous parvenons à ce but nous pourrions envisager entre autres une géométrie sur des objets discrets dans laquelle on raisonne et on calcule rigoureusement. Son cadre pourrait être celui de la Géométrie des Nombres c'est à dire un produit cartésien de l'ensemble des entiers relatifs par lui-même, i.e.  $\mathbb{Z}^n$ . Leurs propriétés devraient les rapprocher de celles des objets euclidiens usuels tout en offrant la possibilité d'évaluer la différence qui les en sépare. Ceci suppose en premier lieu de revoir la notion de réel et de la remplacer par une notion plus pauvre en quantité d'information et de construire des objets géométriques dont la quantité d'information soit également contrôlée.

## II UNE NOUVELLE APPROCHE DES RELATIONS DISCRET-CONTINU

### 1 Atomisme et ordres de grandeur.

Décrivons maintenant les contours d'une voie nouvelle vers ces questions. Les nombreux exemples que nous développerons dans les chapitres suivants montreront qu'elle est effectivement utilisable et qu'elle résoud de nombreux problèmes pratiques. Commençons par quelques remarques générales sur les relations entre le Discret et le Continu.

La thèse usuelle résumée ci-dessus suppose que le continu préexiste et que nous le subdivisons si nous voulons descendre dans l'infiniment petit. La possibilité offerte par l'Analyse Non Standard de manier rigoureusement des ordres de grandeur va nous permettre de renverser ce mécanisme et d'envisager le continu comme un ensemble de relations de voisinages (quasi-topologie) plaquée sur une structure sous-jacente atomique. Ici le discret préexiste et le continu est un changement d'échelle ou un regroupement d'atomes. Un exemple de telle structure est donné par les sous-ensembles des points de  $\mathbb{Z}^n$  contenus dans des fenêtres, (i.e. des parallélépipèdes), de taille entière  $\omega$ . Il n'y a apparemment rien de changé à la thèse usuelle à ceci près que nous **supprimons la possibilité de subdiviser ad infinitum** et qu'il est possible de tirer quelques avantages de la situation. Décrivons en brièvement quelques-uns; la suite de notre travail précisera ces points de bien des façons.

Le premier avantage réside dans le contrôle de la transition Discret-Continu effectué par un paramètre entier  $\omega$ . Ainsi pour tout entier  $\omega$  **standard** la quasi-topologie est la topologie discrète (toute partie est ouverte ou fermée) et pour  $\omega$  **infiniment grand** elle équivaut à la topologie ordinaire des espaces réels. D'une certaine façon rien n'est perdu par rapport aux théories classiques (Analyse, Topologie, Géométrie) qui peuvent être traduites dans ce cadre; elles deviennent des théories simultanément discrètes et continues et plus précisément la proportion de l'un ou l'autre aspect est contrôlable par un paramètre.

Le deuxième avantage réside dans le fait que toute discrétisation se traduit également en termes arithmétiques, les droites sont remplacées par  $\mathbb{Z}$ , les espaces  $\mathbb{R}^n$  par  $\mathbb{Z}^n$ , etc. Tout problème de continuité donne donc naissance à un problème de quasi-continuité (ou s-continuité) mais également à un problème d'arithmétique. Par exemple l'étude classique de la convergence d'une suite réelle donnera ici un problème (en général équivalent) de s-convergence mais amènera aussi la question plus précise de son comportement explicite au voisinage de sa limite. Cette étude se justifie lorsque ce comportement fin est indispensable. D'autre part notre approche met l'outil arithmétique à disposition des applications pratiques.

L'un des souhaits émis plus haut pour harmoniser les aspects discrets et

continus de la Géométrie consiste à essayer de ne pas charger trop vite en quantité d'information les nombres destinés à décrire l'espace. Nous aimerions que la charge informative de l'espace et celle de ses points restent toujours comparables. Un moyen a déjà été proposé il y a fort longtemps par Jean Bernoulli qui utilisait une construction simultanée et progressive du point et de l'espace inspiré de la notion de développement décimal. Son argument est le suivant: si nous connaissons les nombres décimaux de la forme  $\frac{k}{10}$  où  $k$  est entier nous en déduisons une connaissance partielle des droites du plan, par l'intermédiaire des points de meilleure approximation de la grille discrète formée par l'ensemble des points  $(\frac{k}{10}, \frac{\ell}{10})$  où  $(k, \ell) \in \mathbb{Z}^2$ . En réitérant le processus, ie en subdivisant continuellement de la sorte nous pouvons approcher d'aussi près que nous voulons ces droites. Si en plus nous pouvons décrire la structure des approximations nous en déduisons un dévissage progressif de la structure des droites continues limite. Bien sûr l'enjeu ici n'est pas tant de passer à la limite mais d'avoir un objet limite convenable dont nous connaissons les discrétisations. Jean Bernoulli était guidé par des préoccupations de temps de calcul, (c'est aussi l'une des nôtres dans le Calcul en Nombres Entiers) et avait élaboré "une nouvelle espèce de calcul" (cf [4]) basé sur ces suites des meilleures approximations entières d'objets; les lois arithmétiques sous-jacentes à ce processus permettent d'en accélérer le déroulement. Si son calcul ne s'étendait guère au delà de l'accélération des calculs des interpolations linéaires il avait néanmoins parfaitement compris que les objets discrets ainsi définis possèdent des propriétés arithmétiques ("périodes") remarquables. Il a énoncé et rendu praticables quelques-unes de ces lois s'appliquant aux droites discrètes de meilleure approximation entière; il faut attendre Christoffel [22], Markov [71], Venkov [116], pour trouver des énoncés plus précis et leurs preuves. Le sujet est encore loin d'être épuisé (cf. [5], [27], [38], [71], [89], [90], [91], [105]).

Par construction le passage du Discret au Continu s'effectue en un nombre fini d'étapes ce qui peut parfois permettre de suivre l'évolution d'un problème entre ces deux extrêmes. Généralement la finitude est un avantage théorique important si les applications pratiques sont en vue.

Le dernier avantage se trouve dans le grand nombre de façons que nous avons d'introduire des notions de **points** dans l'espace. Ce seront soit les atomes sous-jacents ou des groupes d'atomes, par exemple tous les sous-ensembles assez gros (contenant un disque de rayon  $\rho$  infiniment grand mais infiniment petit devant le paramètre  $\omega$ ). Cette possibilité commande directement les divers passages à la limite dont nous pouvons avoir besoin.

## 2 Le modèle finitaire et le Discret Idéal

Ces principes généraux étant exposés montrons comment les satisfaire. Dans [55] Harthong a introduit l'idée d'un modèle finitaire des réels; il a depuis été utilisé de diverses manières en particulier par Reeb ([93]) pour l'intégration numérique d'équations différentielles. Rappelons cette idée.

Le modèle finitaire du corps des réels est la structure obtenue en munissant, pour un entier infiniment grand  $\omega$  donné, un intervalle  $[-\rho, \rho]$  de l'anneau  $\mathbb{Z}$  d'une **quasi-topologie** via la définition suivante:

$$i \approx j \Leftrightarrow |i-j| \text{ est infiniment petit devant } \omega$$

$\rho$  étant lui-même un entier infiniment grand devant  $\omega$ . Nous désignons par  $\mathbf{R}_{\omega, \rho}$  cette structure.

Il est possible de montrer que des choix d'entiers infiniment grands  $\omega$  distincts conduisent à des quasi-topologies équivalentes à celle d'un intervalle usuel infiniment grand de  $\mathbb{R}$ . Toutes les notions d'analyse classique peuvent être traduites dans  $\mathbf{R}_{\omega, \rho}$ . Le paramètre  $\omega$  doit être compris comme un facteur de grossissement d'une structure apparemment continue et qui devient discrète à cette échelle. Ceci revient à travailler au niveau atomique ou microscopique et à créer les objets à partir de ces briques élémentaires que sont les nombres entiers. Si nous supposons le paramètre  $\omega$  entier ordinaire (i.e. **standard**) la quasi-topologie est la topologie discrète; la transition discret-continu est entièrement contrôlée par le paramètre entier  $\omega$ . Le choix de  $\rho$  permet d'embrasser des parties plus ou moins grandes du corps des réels. Nous désignerons par **théorie discrète idéale** la traduction d'une théorie dans un modèle finitaire de  $\mathbb{R}$ .

En utilisant les ressources de l'Analyse non Standard, il est possible d'introduire des modèles finitaires du corps des réels dans lesquels nous pourrions replacer rigoureusement toutes les théories mathématiques élémentaires: Analyse, Géométrie, Topologie etc. La continuité, la différentiabilité ou toute autre notion "régulière" serait traitée par des considérations d'ordres de grandeur de paramètres arithmétiques. Le plus grand avantage étant, lors d'un traitement numérique, qu'il n'est plus nécessaire de rediscrétiser le continu qui a servi pour modéliser un phénomène; la discrétisation se fait sans erreurs.

## 3 L'hyperordinateur

L'examen d'une variante de ce modèle, sorte d'ordinateur théorique pouvant traiter simultanément les calculs numériques et des notions plus abstraites, comme les relations topologiques, recentre le rapport discret-continu autour du fonctionnement et de l'utilisation d'une machine. L'hyperordinateur est

constitué de deux dispositifs:

- a) un processeur infiniment puissant capable d'effectuer rigoureusement les quatre opérations sur les entiers de l'intervalle  $[0, \omega-1]$ .
- b) une mémoire capable d'enregistrer un entier quelconque de l'intervalle  $[0, \omega^2]$  et les circuits logiques nécessaires à l'évaluation et au transfert dans cette mémoire du produit  $i \cdot j$  de deux entiers de  $[0, \omega]$  d'une part ainsi qu'au calcul du quotient du contenu de cette mémoire par un entier de  $[0, \omega]$ .

L'implémentation complète du modèle finitaire  $\mathbf{R}_{\omega, \rho}$  de  $\mathbb{R}$  dans l'hyperordinateur revient à réaliser une "virgule fixe" utilisant ces données technologiques. En simplifiant il s'agit de pouvoir effectuer les quatre opérations suivantes où  $i$  et  $j$  sont à présent dans l'intervalle  $[-\rho, \rho]$ :

- o La somme:  $(i, j) \longmapsto i+j,$
- o la différence:  $(i, j) \longmapsto i-j,$
- o le produit:  $(i, j) \longmapsto [ij/\omega]$
- o le quotient:  $(i, j) \longmapsto [\omega i/j]$

(dans ce modèle le nombre réel unité, i.e. 1, est représenté par  $\omega$ ).

Pour cela nous choisissons d'abord une valeur de  $\rho$  fixant la puissance de notre machine; à la fois par simplicité et pour des raisons théoriques nous prenons  $\rho = \omega^2$ . A partir de là nous travaillons en base  $\omega$  avec des nombres à deux chiffres  $\pm x_1, x_0$  représentant les entiers  $x_1 \omega + x_0$  de  $[-\omega^2, \omega^2]$ . La réalisation pratique usuelle de cette virgule fixe utilise ce découpage des nombres et ramène le traitement des quatre opérations précédentes à des calculs portant sur les chiffres, soumis au processeur, et aux ajustements des retenues confiés à une circuiterie ou à un logiciel spécialisés. Que le nombre de chiffres généralement trop grand ou que le confort des réels aient créé des habitudes la gestion des retenues n'a que très rarement été envisagée formellement; nous intégrons sa gestion dans les programmes soumis à l'hyperordinateur. Pour les nombres à deux chiffres ce n'est pas un travail excessif. Cette idée formalise la gestion des retenues introduite par Reeb dans un programme d'intégration entière de l'équation différentielle  $y'=y$  en 1986. Nous désignons par  $H_\omega$  cette machine.

Si les retenues sont gérées dans l'algorithme soumis à l'hyperordinateur il faut, pour évaluer une fonction par exemple, exprimer les chiffres du résultat à l'aide des chiffres de ses variables et paramètres. Autrement dit il faut généraliser les algorithmes des quatre opérations usuelles dans le système décimal. Les formules obtenues font intervenir la fonction partie entière ou troncature. Nous désignons par **calcul en nombres entiers** ou **arithmétisation par troncature** la programmation de l'hyperordinateur.

Malgré toute sa simplicité cette machine est capable de traiter de manière finitaire tout problème de mathématique (voir la théorie IST, [74]). Il serait intéressant de la comparer plus précisément avec les machines de Turing de puissance non standard et de relier notre approche à la théorie des Langages Formels. Les théories discrètes idéales deviennent, dans un sens purement heuristique, les langages spécialisés (topologie, analyse ...) reconnus par l'hyperordinateur. Elle permet de relier le continu au discret idéal.

#### 4 Le contenu des théories discrètes idéales

Un objet discret idéal plongé dans une théorie discrète idéale reflète le caractère particulier des objets standards. C'est une **classe** très vaste contenant toutes leurs discrétisations; elle correspond à un unique objet standard continu. Cette non-unicité des représentants des objets idéaux est à la fois leur force et leur faiblesse.

Bien que notre Géométrie Discrète soit proposée essentiellement pour résoudre les conflits numériques entre discret et continu géométriques, comme beaucoup de théories, elle réserve des surprises. La quasi-unicité en particulier mérite quelques éclaircissements.

Lorsque nous construisons le continu à partir d'une structure discrète il n'y a pas beaucoup de choix en dimension 1, le corps des réels suggère naturellement de s'appuyer, comme nous l'avons fait, sur l'anneau des entiers. Il n'en n'est plus de même pour les dimensions supérieures. Si nous avons choisi de construire le continu à partir de  $\mathbb{Z}^2$  c'est avant tout pour avoir la structure discrète la plus simple possible et parce que la technologie l'utilise largement. Mais nous pourrions remplacer  $\mathbb{Z}^2$  par d'autres groupes discrets. Autrement dit la liaison discret-continu peut relier un groupe discret et un groupe continu. Le premier possède en général une structure beaucoup plus frustrante que le dernier; ainsi lorsqu'un objet transite de la théorie construite sur le groupe discret vers la théorie continue il doit s'équiper progressivement des attributs nécessaires à sa vie dans le nouveau monde. Mais cet enrichissement dépend de l'objet qui voyage même si ces objets aboutissent au même but dans le monde continu; il est donc nécessaire d'identifier tous les objets qui tombent sur un objet continu bien défini. Réciproquement l'objet continu pourra retourner dans le monde discret par l'un des éléments de la classe d'équivalence correspondante. La notion de point est également soumise à ces lois.

Donnons un exemple à partir des transformations affines du plan. Le transport d'une fonction affine contractante du plan continu dans son modèle discret,  $\mathbb{Z}^2$ , conduit tout naturellement aux applications de  $\mathbb{Z}^2$  dans  $\mathbb{Z}^2$ , que nous

appelons quasi-affines, définies comme suit ([] est la partie entière):

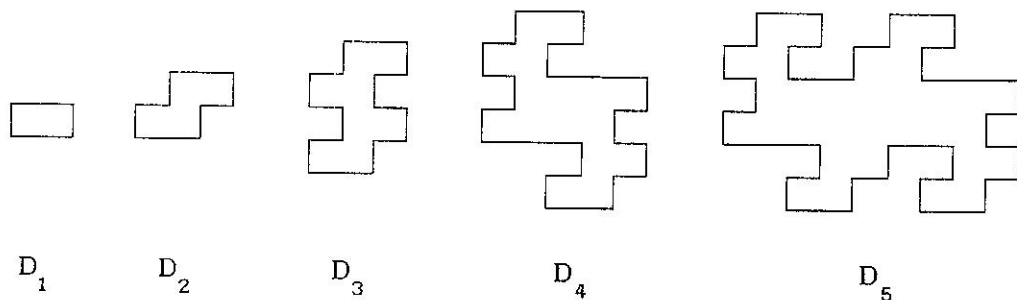
$$(\phi) \quad \begin{cases} X' = \left[ \frac{aX+bY}{\omega} \right] \\ Y' = \left[ \frac{cX+dY}{\rho} \right] \end{cases}$$

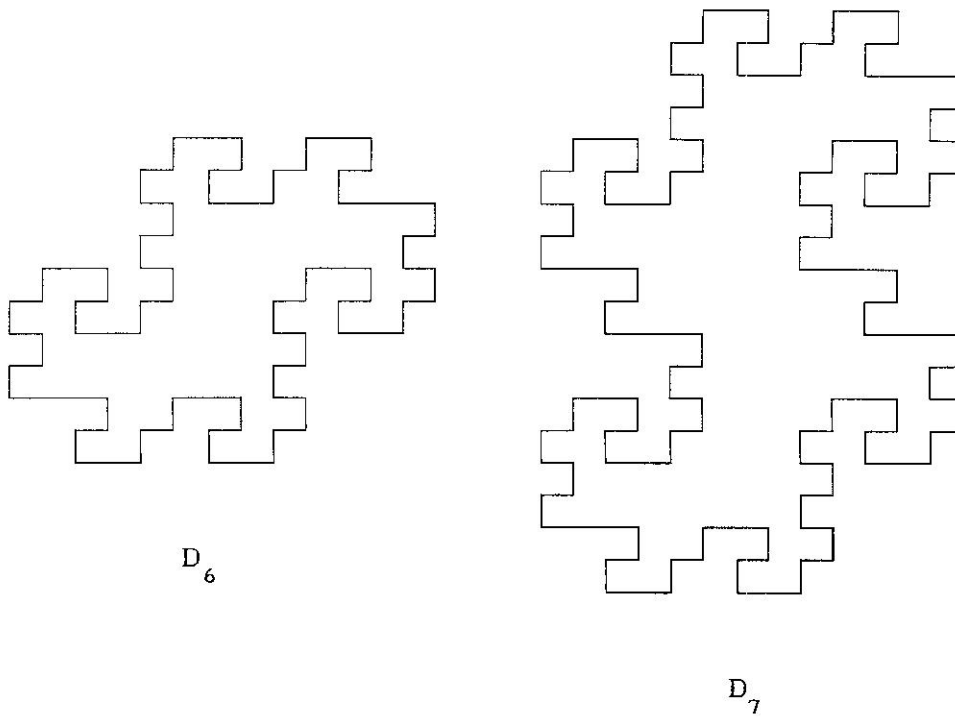
où  $a, b, c, d$  sont des entiers et  $\omega$  et  $\rho$  sont des entiers positifs vérifiant  $\rho\omega > |ad-bc|$ ; les deux derniers paramètres  $\omega$  et  $\rho$  étant ceux du passage à la limite qui s'effectue simplement en considérant  $\omega, \rho, X$  et  $Y$  infiniment grands. Ces paramètres jouent le même rôle que l'épaisseur  $\omega$  des droites discrètes précédentes. Nous pouvons montrer que dans ce passage à la limite les transformations quasi-affines redonnent les applications affines et vérifier que leurs propriétés redonnent bien celles des transformations affines. Mais ces objets et leurs propriétés existent tant à l'échelle microscopique ( $\omega, \rho, X$  et  $Y$  ordinaires) qu'à l'échelle du passage à la limite ( $\omega, \rho, X, Y$  infiniment grands), leur définition ne dépendant que de paramètres entiers. En particulier les transformations quasi-affines ne sont pas en général bijectives même si leur "limite" le sont, elles possèdent peu de symétries strictes même si leurs limites en ont beaucoup etc... Ces conflits se résolvent grace à la tolérance due à la quasi-unicité. Ceci provoque le développement de caractères étranges toujours fascinants à regarder. Montrons que l'état **fractal** est pratiquement une conséquence de cette quasi-unicité appliquée au monde des transformations quasi-affines.

En prenant  $a=1, b=1, c=-1, d=1$  et  $\omega=\rho=2$  voici quelques images réciproques

$$D_k = \phi^{-k}(0) \quad (1)$$

de l'origine pour les premières valeurs de  $k$ ; nous reconnaissons les célèbres courbes du Dragon de Mandelbrot (cf [70]).





Les courbes du Dragon  $D_k$ ,  $k=1, \dots, 7$ .

fig. 3

L'équation (1) constitue donc une équation de ces courbes fractales dont nous pouvons déduire la plupart de leurs propriétés. Il est intéressant d'observer l'évolution, lorsque  $k$  augmente, de certains aspects de la transformation quasi-affine

$$\begin{aligned} X' &= \left[ \frac{X+Y}{2} \right] \\ Y' &= \left[ \frac{-X+Y}{2} \right] \end{aligned} \tag{2}$$

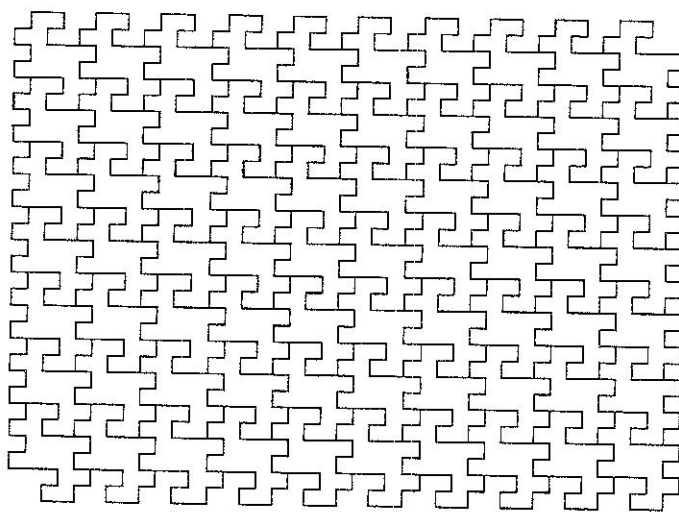
vers des propriétés de la transformation linéaire

$$\begin{aligned} X' &= \frac{X+Y}{2} \\ Y' &= \frac{-X+Y}{2} \end{aligned} \tag{3}$$

Il est facile de montrer que l'application (2) induit, pour tout  $k \geq 0$ , un pavage de  $\mathbb{Z}^2$  en  $D_k$  comme sur les figures 4 et 5 suivantes qui représente ceux pour lesquels  $k=4$  et  $k=5$ . Il faut observer sur le dernier que le regroupement des  $D_5$  n'est pas le pavage trivial que l'on peut former en juxtaposant les  $D_5$  en lignes et en colonnes.

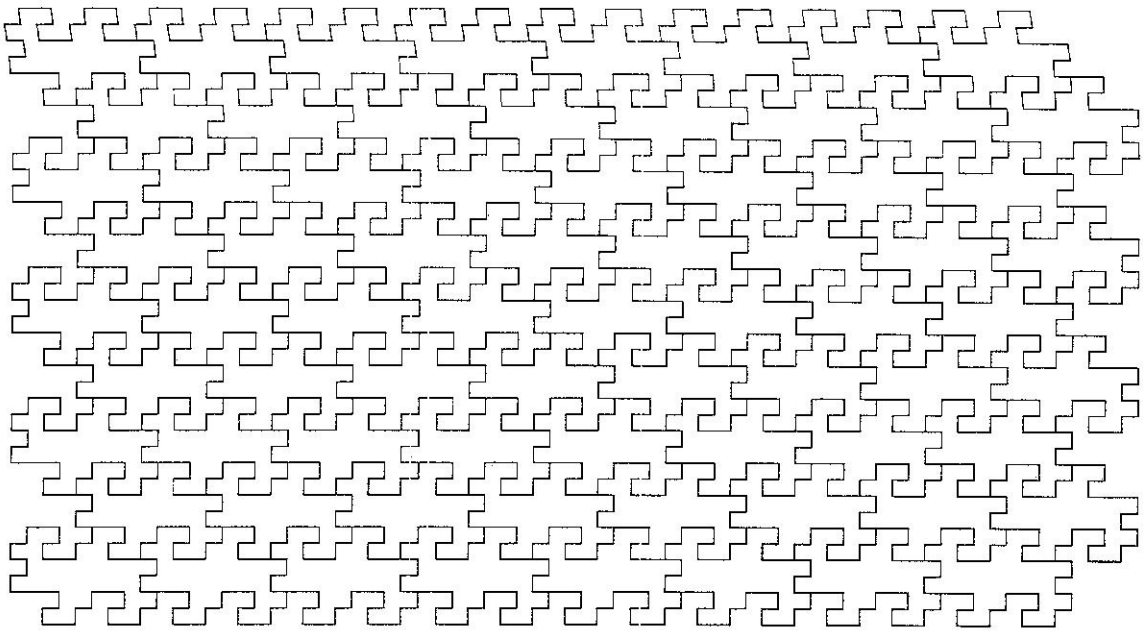
D'autre part (2) s'étend canoniquement en une application  $f$  définie sur le pavage en  $D_{k+1}$  et à valeur dans le pavage en  $D_k$ . La figure 6 indique, à l'aide

de  $D_5$  et  $D_4$ , l'action de cette transformation: le pavé "0" du premier donne le pavé "0" du deuxième etc... Nous voyons que le segment AB contenu dans le contour associé à  $D_5$  est transformé dans le segment A'B' dans  $D_4$ . L'angle de  $-\frac{\pi}{4}$  et le rapport d'homothétie de  $\frac{\sqrt{2}}{2}$  de (3) sont bien au rendez-vous et le restent pour toute valeur de  $k \geq 1$ . Le seul défaut de  $f$ , pour ainsi dire, vient de ce que sa source et son but ne sont pas le même espace. Si nous introduisons la quasi-topologie du §6 sur  $\mathbb{Z}^2$  pour un entier infiniment grand  $\omega$  tous les dragons  $D_k$  où  $k$  est i.p. devant  $\omega$  deviennent des points: les pavages en  $D_{k+1}$  ou en  $D_k$  héritent de structures quasi-topologiques équivalentes; ils représentent alors le même espace (un modèle finitaire de  $\mathbb{R}^2$ ). Nous voyons comment le problème discret posé par la transformation (2) à fait apparaître une nouvelle partition en "points" de la structure sous-jacente  $\mathbb{Z}^2$ . Cette nouvelle notion de point est parfaitement compatible avec celle que l'on fait apparaître en considérant l'intersection de deux droites épaisses. Ces points  $D_k$  pour  $k$  i.g. peuvent alors être considérés comme des invariants simultanés de (2) et (3). Leur caractère fractal provient de ce double héritage.



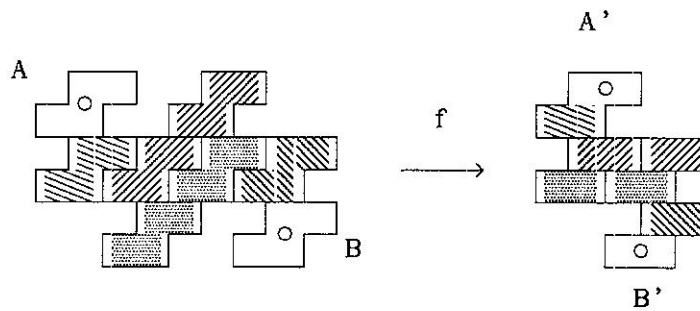
Le pavage en  $D_4$ .

fig. 4



Le pavage en  $D_5$ .

fig. 5



La transformation  $f$  de  $D_5$  dans  $D_4$ .

fig. 6

### III UTILISATION PRATIQUE DE LA NOUVELLE APPROCHE DISCRET-CONTINU.

Le discret idéal repose sur l'emploi de paramètres pouvant prendre des valeurs inaccessibles aux ordinateurs (entiers infiniment grands). Bien que la conversion d'objets continus en objets discrets fournisse beaucoup de représentants des objets discrets idéaux, leur emploi effectif en machine nécessite d'en connaître le plus de propriétés possible, ce qui restreint fortement les possibilités. Seuls certains représentants simples, dont les propriétés sont connues pour toute valeur des paramètres, seront retenus. Dans ce § nous précisons cette question en sachant bien que nous ne pouvons guère dépasser le stade de l'heuristique.

## 1 La chaîne d'hyperordinateurs

Deux hyperordinateurs de puissances entières infiniment grandes  $\omega$  et  $\omega-1$  ont des langages  $\mathcal{L}_\omega$  et  $\mathcal{L}_{\omega-1}$  "équivalents"; chacun comprend l'autre à des détails près. Les langages de  $H_\omega$  et  $H_{\omega-1}$  sont "infiniment voisins". Nous pouvons alors envisager la chaîne finie constituée par tous les hyperordinateurs  $H_\omega, H_{\omega-1}, \dots, H_1$ . Si  $n$  est un entier standard,  $H_n$  est donc un ordinateur usuel capable de comprendre un langage standard  $\mathcal{L}_n$  qui est une partie de la mathématique discrète. Dans ce réseau chaque machine comprend assez bien ses voisins immédiats mais moins bien les voisins éloignés. Il est analogue à ce que serait peut-être l'état linguistique du globe si sa surface était homogène et si ses populations avaient évolué en restant sédentaires. Pour les valeurs standard de  $n$  les langages  $\mathcal{L}_n$  sont ceux d'ordinateurs usuels et leur réunion décrit le champ de la Mathématique Discrète. Même s'il n'est pas possible de décrire tous les détails des relations entre ces langages leur simple considération suffit à resituer le débat discret-continu sur des bases très fécondes.

L'existence de cette chaîne nous permet d'envisager différemment le contenu des Mathématiques Discrètes Idéales et leurs relations avec les Mathématiques Discrètes ordinaires. En effet chaque Théorie Discrète Idéale est indexée par un entier infiniment grand et reliée par une chaîne de Théories analogues dont les indices décroissent d'une unité à chaque fois jusqu'à celles d'indices standard, éventuellement à celle d'indice 1; cette dernière est triviale. C'est en ce sens que nous dirons que les Théories Discrètes sont paramétrées. Ces chaînes de Théories Discrètes sont équivalentes, à leur extrémité non-standard, à des Théories Continues et à des Théories vraiment Discrètes à l'autre. Si une Théorie peut être construite sur ce principe ses notions, ses théorèmes sont également connus tout au long de la chaîne. Par conséquent elle permet de relier explicitement des mondes analogues qui existent sous forme discrète ou continue. Les notions ou propriétés seront discrètes standard (par exemple arithmétique) à une extrémité et réelles (ou topologiques) à l'autre.

## 2 Avantages des objets discrets paramétrés.

Cette vision des relations entre Mathématiques Discrètes Idéales et Mathématique Discrète a de nombreux avantages, l'essentiel étant que les Théories Discrètes Idéales possèdent simultanément les vertus des deux mondes antagonistes continu et discret. Pour un spécialiste du discret qui cherche à organiser son territoire, le plongement de ses objets dans des familles paramétrées l'amènera, par la considération des relations que le continu impose aux extrémités non-standard de ces familles, à mieux comprendre leurs

caractéristiques propres. Dans ce sens les structures du continu peuvent être suivies et perçues jusque dans le monde discret. La recherche des familles discrètes paramétrées demande de sélectionner dans les classes idéales, qui sont constituées de toutes les discrétisations d'un objet continu, les représentants les plus avantageux pour le problème à résoudre. De nombreux choix sont possibles pour élaborer ces chaînes; nous pouvons commencer leur construction à partir du continu ou du discret ou des deux à la fois.

Cette approche explique aussi pourquoi beaucoup de théories discrètes différentes peuvent aboutir à la même théorie idéale et avoir la même trace macroscopique continue.

Les mathématiques du Continu réalisent un accord parfait entre le nombre et la forme; celui-ci se détruit dès que l'on quitte ce territoire idéal pour les mathématiques finies. La "continuité" des chaînes paramétrées devient intéressante pour suivre l'évolution du désaccord entre les calculs analytiques et les propriétés géométriques au fur et à mesure de cet éloignement.

### 3 Les relations entre les Théories Discrètes et les Théories Discrètes Idéales

Affinons notre description du mécanisme des relations entre le Discret Idéal et le Discret standard. La question consiste à savoir comment sélectionner les bons représentants des objets des Théories Discrètes Idéales. Ceux-ci relient le plus directement et le plus simplement possible leurs analogues discrets et continus. Par exemple il est facile d'envisager de nombreuses définitions de droites discrètes construites sur  $\mathbb{Z}^2$ ; il suffit que chacune d'elle redonne la notion de droite usuelle par trace macroscopique; toutefois la restriction de ces notions au domaine discret standard n'est en général pas intéressante. Les Mathématiques Discrètes standard n'utilisent qu'un très petit nombre d'objets "intéressants" qui ne sont pas immédiatement repérables dans les classes formées par nos objets idéaux; ce sont eux les objets simples sur lesquels nous devons nous appuyer. Comme le paramétrage arithmétique des modèles finitaires  $R_{\omega,\rho}$  permet de transporter toute notion du champ de la Mathématique discrète et à celui de la Mathématique Discrète Idéale et réciproquement, un certain nombre d'allers et retours entre les deux territoires permettent en général de dégager les bonnes notions. De façon générale la Mathématique Discrète sélectionnera les meilleurs représentants des classes idéales mais la considération de représentants différents, en un certain sens voisins, et de leurs prolongements dans le territoire Idéal permettra, en retour d'enrichir ou de mieux cerner les objets discrets initiaux. Les Théories Discrètes Idéales contribuent par ce biais à enrichir

les Mathématiques Discrètes usuelles.

Par exemple les définitions de courbes discrètes couramment admises en Topologie Discrète, trop rigides, conduisent dans certains usages à des effets secondaires désagréables: clignotements dans les animations, effets de moirés (aliassages) dans les transformations. Le premier effet apparaît si nous voulons déplacer une droite sur un écran parallèlement à elle-même en utilisant un feuilletage discret formé de droites disjointes. L'observation que les droites discrètes sont également les solutions d'équations différentielles en nombres entiers conduit à un algorithme d'animation "douce" beaucoup plus agréable à l'oeil.

Le point essentiel dégagé ici peut s'énoncer comme suit:

**Les classes d'objets introduites par la Mathématique Discrète Idéale persistent dans la Mathématique Discrète Standard.** Si plusieurs représentants d'un objet idéal sont placés dans des familles paramétrées d'objets qui les relient au monde discret usuel leurs instanciations pour une même valeur standard du paramètre crée des objets discrets indirectement liés même si leur cousinage n'est pas immédiatement apparent. Par cette méthode nous pouvons découvrir des relations cachées entre des notions discrètes différentes qui permettent de mieux les comprendre et de les utiliser plus efficacement. En particulier il est parfois plus aisé de découvrir des cousinages entre certaines notions discrètes par la considération des relations qui existent entre leurs prolongement idéaux; la considération de leurs analogues continus pouvant être stérile.

#### 4 Applications algorithmiques de l'hyperordinateur: Le Calcul en Nombres Entiers.

Si nous utilisons effectivement sur ordinateur standard, où tout au plus  $\omega$  vaudra  $2^{32}$  voir  $2^{64}$ , des programmes écrits pour l'hyperordinateur, ces programmes perdent leurs propriétés topologiques mais conservent leur pouvoir numérique. L'endroit où sont traitées les retenues, (le programme, le compilateur ou le silicium) a peu d'influence sur la précision des résultats à condition qu'elles le soient. Pourtant il est surprenant de constater à quel point le fait d'intégrer cette gestion dans les programmes en accélère l'exécution; nous avons observé des divisions par des facteurs 100 des temps de calculs. Nous verrons dans les deuxième et troisième parties combien cette méthode est utile dans l'étude théorique des relations entre le discret et le continu.

le Calcul en Nombres Entiers permet donc de convertir des algorithmes "réels" en algorithmes "entiers"; donnons-en ici un avant-goût avec le traitement de l'équation différentielle mentionnée ci-dessus.

L'arithmétisation de la fonction exponentielle.

En considérant la fonction exponentielle comme la solution de l'équation différentielle

$$y' = y \quad (1)$$

valant 1 pour la valeur 0 de la variable  $x$  nous arithmétisons la méthode d'intégration d'Euler de la façon suivante.

Subdivisons l'intervalle  $[0,1]$  en parties égales par les points  $x_i = \frac{i}{\omega}$  et désignons par  $\eta_i$  la valeur en  $x_i$  de la solution étudiée. La dérivée étant

approchée par l'expression  $\frac{\eta_{n+1} - \eta_n}{1/\omega}$  nous ne commettons qu'une erreur

infinitement petite en appliquant à  $\eta_n$  une homothétie de rapport infinitement grand  $\omega$  suivie de la troncature

$$Y_n = [\omega \eta_n] \quad (2)$$

ce qui remplace l'équation (1) par la relation

$$\omega Y_{n+1} = \omega Y_n + Y_n \quad (3)$$

où  $Y_n$  est la solution (entière) inconnue. Exprimons l'entier  $Y_n$  dans la base de numération  $\omega$  sous la forme

$$Y_n = c_1 \omega + c_0 \quad (4)$$

où  $c_0$  et  $c_1$  sont des chiffres. En reportant dans (3) nous trouvons

$$\omega Y_{n+1} = c_1 \omega^2 + (c_0 + c_1) \omega + c_0 \quad (5)$$

d'où nous tirons les deux premiers chiffres de  $Y_{n+1}$  désignés par  $c'_0$  et  $c'_1$ :

$$\begin{aligned} c'_0 &= \{c_0 + c_1\} \\ c'_1 &= c_1 + [c_0 + c_1] \end{aligned} \quad (6)$$

où, pour alléger les notations  $\{c\}$  (resp.  $[c]$ ) désigne  $c \bmod \omega$  (resp.  $c \div \omega$ ) c'est à dire le reste et le quotient de la division euclidienne de  $c$  par  $\omega$ .

Ces relations de récurrence expriment les chiffres de  $Y_{n+1}$  lorsqu'on connaît ceux de  $Y_n$ . Ces deux relations constituent le traitement en nombres entiers de la méthode d'Euler. La suite  $\frac{c_1}{\omega} + \frac{c_0}{\omega^2}$  est infinitement voisine de la suite  $\exp(n/\omega)$ .

Si nous appliquons la récurrence (6) avec un  $\omega$  ordinaire nous constatons à la fois une bonne précision et une grande rapidité dans l'exécution. Ces qualités donnent un grand intérêt pratique à toute généralisation de cette méthode.

Le Calcul en Nombres entiers traduit l'algorithme initial en relations entre les chiffres dans une base de numération des diverses grandeurs qui interviennent; en libérant les chiffres, il devient une abondante source

d'algorithmes.

## 5 L'émergence d'une théorie: la Géométrie Discrète

Pour nous faire une opinion de la pertinence et de la portée de notre approche du thème **discret idéal-discret** nous avons cherché un terrain d'essai où les objets définis par le calcul en nombres entiers satisfassent aux exigences que nous venons d'énoncer, en particulier qu'ils prolongent des objets déjà existants en mathématique discrète. Un tel raccord se produit dans le domaine de l'**Algorithmique Graphique**: les droites discrètes obtenues par le calcul en nombres entiers sont liées à celles que donne l'algorithme de Bresenham (cf. [10]) introduit pour le tracé sur écran discret. Ce dernier génère les points entiers les plus voisins d'une droite rationnelle donnée. L'approche en nombres entiers permet de retrouver cet algorithme par voie purement arithmétique et montre comment définir une notion de droite discrète valable dans les mondes discret et discret idéal. Autant qu'une confirmation des algorithmes en nombres entiers c'est l'existence d'une géométrie discrète, convergeant vers la géométrie euclidienne, qui est ainsi révélée.

La deuxième partie de ce travail est consacrée aux premiers pas dans l'étude de cette Géométrie et concerne essentiellement les droites discrètes. Nous y montrons qu'elles ne sont qu'une traduction **géométrique** du groupe modulaire et que cette traduction ne **pénalise** pas l'algorithmique, au contraire. Nous obtenons un grand nombre de théorèmes de structures et d'algorithmes les concernant et obtenons des résultats nouveaux. Quelques propriétés élémentaires avaient été découvertes dans les deux dernières décennies par des spécialistes d'informatique graphique (cf. [12], [17], [34], [35], [39], [61], [69], [80], [81], [82], [121]). Leurs méthodes, contrairement aux nôtres, occultaient complètement le rôle joué par l'arithmétique. Cette dernière apporte pourtant une généralité et une efficacité incomparables.

Disons brièvement qu'une droite discrète est l'ensemble des points entiers d'une bande rationnelle et que cette notion dépend d'un paramètre entier: l'**épaisseur arithmétique**  $\omega$ . C'est le lien cherché entre les domaines discret et discret idéal. Sans que ceci décrive le contenu de la deuxième partie disons que sur ces droites on définit des relations de parallélisme, d'orthogonalité, des symétries, qu'on peut étudier l'ensemble des droites passant par deux points, l'intersection de deux droites, la notion de segment, les inclusions de segments, la convexité, la dualité etc... Cependant leurs propriétés sont sensiblement différentes de celles de la géométrie usuelle;

par exemple, deux droites discrètes distinctes peuvent, si leur épaisseur est petite, ne s'intersecter en aucun point, comme des diagonales orthogonales noires et blanches d'un échiquier; toutefois leur intersection sera non vide si leurs épaisseurs sont des **entiers infiniment grands**.

La présence du paramètre entier  $\omega$  dans la notion de droite n'est pas un inconvénient. En le choisissant convenablement nous obtenons plusieurs notions de droites (8-connexes, 4-connexes,...) déjà utilisées par les spécialistes. D'autre part un peu de réflexion montre que la Géométrie Discrète de dimension 3 ou plus réclame obligatoirement une notion de droite d'épaisseur variable.

Rappelons à ce propos l'aspect général des relations entre les notions continues et discrètes que nous avons soulevé à propos des Théories Discrètes Idéales: une notion continue donne naissance à plusieurs notions discrètes analogues (et souvent beaucoup). Mais toutes sont des instanciations d'une même notion. Il existe de même plusieurs notions de cercles discrets, plusieurs notions de rotation discrète (nous en présentons trois dans le chapitre qui leur est consacré), plusieurs notions de convexité... Aucune des notions discrètes correspondant à une notion continue ne possède **toutes** les propriétés de son équivalent continu mais chacune a ses avantages: l'art de la Géométrie Discrète consiste à les organiser les unes par rapport aux autres, à transférer les propriétés du continu à des objets qui ne peuvent pas les vérifier.

Tous les spécialistes des méthodes discrètes savent bien que cette dualité discret-continu n'est pas quantifiable; ils s'y réfèrent pourtant constamment. A travers les paramètres entiers et leurs ordres de grandeurs nous ne cherchons qu'à rendre un peu plus effective cette dialectique.

La Géométrie Discrète Idéale qui consiste à étudier les **halos** des objets euclidiens standards: points, droites, plans, cercles,...est **équivalente** à la Géométrie Euclidienne. La description, dans tous ses détails de cette Théorie est sans mystère; elle n'est peut-être pas la première urgence et nous ne l'avons pas incluse dans ce travail. Par contre elle a joué pour nous le rôle important d'horizon théorique dans notre construction de la Géométrie Discrète permettant d'agencer les notions et de mieux cerner leurs interrelations.

Des généralisations diverses sont en cours: courbes discrètes, géométrie discrète dans l'espace etc... avec l'espoir de développer une théorie analogue à la géométrie analytique de Descartes où l'arithmétique entière remplacera les calculs réels.

Les mêmes principes semblent réutilisables pour établir des liaisons de même nature entre le discret et le continu (topologie, éléments finis, etc...) permettant d'exploiter plus efficacement les avantages de chaque domaine.

## 6 La coexistence avec d'autres théories discrètes.

La structure des données discrètes sur lesquelles on travaille joue un rôle primordial dans l'élaboration des théories discrètes. Toute notion affine ou euclidienne est convertible, en général de plusieurs façons, en Géométrie Discrète, redonnant la notion classique si nous retournons en Géométrie Euclidienne; nous avons longuement parlé de cette quasi-équivalence entre les deux théories. Dans son travail le géomètre discret dispose de toutes les ressources des nombres qui lui permettent de travailler **au pixel près**. Bien sûr la quasi-unicité l'obligera à devoir faire des choix: la sélection des meilleurs objets discrets en priorité, à notre avis, parmi tous ceux qui ont été apportés et étudiés au sein de la science du discret: Combinatoire, Informatique etc. Mais cette Géométrie Discrète suppose des données régulières, conformes au groupe  $\mathbb{Z}^n$ . Que faire si le domaine d'intérêt ne comporte que des structures irrégulières? C'est ici que l'on voit vraiment la nécessité de la quasi-unicité. La Géométrie Discrète Idéale s'accommoderait parfaitement de notions de droites beaucoup plus souples que celle que nous proposons et dont les points seraient alignés **en moyenne**; cette nouvelle notion serait certainement bien adaptée aux situations discrètes stochastiques. Nous pouvons penser qu'il existe une Géométrie Discrète Stochastique qui vient également se raccorder à la Géométrie Discrète Idéale; à partir de là les deux théories convergent vers la Géométrie Euclidienne en étant assez peu distinctes l'une de l'autre. C'est, évidemment, dans la première partie de leur existence, entre le fini standard et le fini non standard qu'elles sont nettement séparées. Ces quelques perspectives, peut-être concrétisées dans le futur, ne sont évidemment qu'une partie des richesses entrevues au travers de l'existence d'entiers infiniment grands.

DEUXIEME PARTIE

LA GEOMETRIE DISCRETE

## INTRODUCTION

Présentons d'abord cette géométrie, non-euclidienne vue de près et euclidienne vue de loin, destinée à décrire les propriétés des objets quasi-linéaires construits sur des structures discrètes régulières et dont l'élaboration nous permet de tester les mécanismes des Théories Discrètes Idéales.

### Quelques rappels historiques

Au 18<sup>e</sup> siècle Jean Bernoulli avait proposé à ses confrères astronomes, "Une nouvelle Méthode de Calcul" (cf [4]) destinée à accélérer les calculs d'interpolation linéaire en les ramenant à des algorithmes arithmétiques étonnamment simples. Partant du fait que l'ensemble des points décimaux du plan est la suite des homothétiques, dans les rapports  $10^{-k}$ , de la grille des points entiers, ceci permet de remplacer les points d'une droite  $D$  par une suite de droites discrètes formées par les points entiers les plus voisins de  $D$  dans chacune de ces grilles. Il découvre alors que toutes ces droites discrètes sont isomorphes; il suffit donc, pour les calculs, d'en connaître une seule. Nous comprenons immédiatement le profit qu'il a pu en tirer pour les interpolations manuelles.

Le patrimoine de Jean Bernoulli s'est évidemment transformé dans les mains de ses héritiers; ils ont retenu de consolider sa charpente initiale, la structure de la droite discrète d'approximation entière par défaut, et de construire immédiatement autour les deux domaines que nous appelons aujourd'hui "Les mots de Sturm" et "Les nombres de Markov". Parmi ces spécialistes, où apparaissent Markoff [71] et indirectement Sturm, nous trouvons entre autres Christoffel [22], Smith [110], Venkov [116], Morse et Hedlung [71], Series [105], Rauzy [91], Dulucq et Gouyou-Beauchamps [38], Berstel [5]. Il nous semble toutefois que ces travaux importants ne sont le développement que d'une petite part des idées de Jean Bernoulli. Peut-être lui prêtons nous plus qu'il faudrait mais nous y voyons l'idée de rechercher les lois arithmétiques que possèdent les objets formés des points de meilleure approximation entière d'entités continues propres à l'analyse ou à la géométrie. Ces règles apparaissent obligatoirement lorsque des théories continues sont astreintes à se développer dans un environnement finitaire ou sont composées avec l'opérateur de troncature.

De façon indépendante, l'apparition des écrans graphiques, les réseaux de processeurs ou d'appareils connectés comme  $\mathbb{Z}^2$  ou  $\mathbb{Z}^3$ , mettent en lumière chaque jour de nouveaux usages des droites de meilleure approximation entière.

Certaines de leurs propriétés ont été redécouvertes par les spécialistes d'Informatique Graphique qui se sont surtout attachés à leurs conséquences

algorithmiques (Rosenfeld [100], Bresenham [10]). Depuis, une grande activité s'est développée dans ce milieu, amenant questions et résultats autour de cette notion. De nombreuses publications décrivent ces travaux, dont nous retenons celles de Hung ([61]), Pham ([80]) et Wu ([120]), parmi les plus significatives.

C'est fortuitement, engagé dans un programme de recherche visant à arithmétiser l'Analyse et la Géométrie à partir du théorème de finitude d'Edward Nelson (cf [74]), que nous avons constaté la proximité de nos vues et du courant décrit ci-dessus. Cette coïncidence a renforcé nos convictions initiales et nous a incité à commencer une synthèse des messages voisins, malgré les distances apparentes, de Jean Bernoulli, Edward Nelson et des constructeurs d'ordinateurs. La traduction de ces discours dans une langue commune, Géométrie Discrète ou Calcul en Nombres Entiers, suggère que parmi les objets discrets certains sont plus simples, plus riches en propriétés théoriques et plus intéressants pour les applications. De là à vouloir les organiser de façon cohérente il n'y a qu'un pas.

Le besoin d'une Géométrie Discrète.

Si nous parcourons la littérature des spécialistes de Géométrie Algorithmique, du Traitement de l'Image et de la Reconnaissance des Formes, de Topologie Discrète, d'Algorithmique Graphique,... nous trouvons à la fois des travaux étiquetés "Géométrie Discrète" et des souhaits pour fonder une telle discipline, ce qui semble contradictoire. Plusieurs points de vue coexistent donc. Pour Rosenfeld [101] par exemple *"Digital Geometry is the study of geometric properties of sets of lattice points produced by digitizing regions or curves in the plane"*. D'autres comme Greene et Yao dans [48] ayant trop souvent rencontré des difficultés à transférer vers l'ordinateur des algorithmes de Géométrie Euclidienne considèrent que *"when the underlying geometric space is intrinsically discrete, as is the case for computer graphics, such algorithms are apt to give invalid solutions if properties of a finite-resolution space are not taken into account"*. Alors que pour le premier la Géométrie Discrète est l'étude de l'ensemble des problèmes liés à la discrétisation des objets continus, les derniers ne se satisfont pas de cette définition et souhaitent un cadre théorique dans lequel ils pourraient dégager les aspects géométriques et algorithmiques de certains objets. Ils proposent d'ailleurs leur solution. Entre ces deux approches nous voyons surtout une différence de tolérance, la première n'accepte que les objets qui sont des discrétisés d'objets continus, la deuxième suggère d'étudier les propriétés des espaces discrets même s'il faut faire apparaître des classes d'objets beaucoup plus riches. Le cœur du débat est là, entre rigorisme et tolérance.

Tous les travaux, et ils sont nombreux (Rosenfeld [97], [98], Forrest [43], Overmars [77], Greene-Yao [48], Chassery [20], [21] ...), relevant de ces deux catégories, indiquent clairement que pour espérer trancher il faut en premier lieu examiner la notion de droite. Qu'est-ce qu'une droite discrète? Est-il possible d'introduire une notion qui puisse englober les approches concrètes, satisfaire les besoins des théoriciens mais aussi être liée avec celle des mathématiciens?

#### Géométrie Discrète et Analyse Non Standard.

Terminons cette introduction par quelques mots précisant les liens existants entre la Géométrie Discrète et l'Analyse Non Standard et quelques commentaires sur les perspectives de la première.

Telle que nous la concevons la Géométrie est une chaîne de Théories reliant la Géométrie Discrète proprement dite, celle du monde réel, des ordinateurs, des applications, à la Géométrie Euclidienne en passant par la Géométrie Discrète Idéale. Elles se distinguent par la puissance des outils qu'elles emploient. La première utilise des ordinateurs ou des entiers standard, la dernière des nombres réels, l'intermédiaire a la possibilité d'utiliser des entiers infiniment grands.

Notre continu est construit sur une structure atomique sous-jacente régulière, (nous nous limitons au cas de  $\mathbb{Z}^n$ ). Nous l'étudions à des échelles différentes, soit de près, soit de loin. Notre idée est de nous en approcher ou de nous en éloigner très progressivement, et non pas de considérer seulement les deux extrémités. La Géométrie devient alors une chaîne continue de théories qui se déforment régulièrement entre les deux pôles extrêmes.

Les objets géométriques sont constitués des points entiers contenus dans des domaines réels usuels: bandes planes pour les droites, parties d'espaces pour les plans, couronnes pour les cercles etc. Il est clair que ces objets discrets ont des propriétés généralement éloignées de celles de leurs analogues continus, mais si les largeurs des domaines considérés sont des entiers infiniment grands, en les remplaçant dans une autre échelle infiniment grande devant ces largeurs, i.e. en les regardant d'encore plus loin, ils retrouvent à des irrégularités négligeables près, un comportement euclidien.

La transition entre les deux faces de la Géométrie s'effectue donc en épaississant progressivement les enveloppes des objets discrets. Le domaine de la Géométrie Discrète Idéale est alors celui des objets d'épaisseur infiniment grande alors que la Géométrie Discrète Arithmétique est celui des objets d'épaisseur standard. Le "passage à la limite" c'est à dire le franchissement de la distance entre la Géométrie Discrète Idéale, où des paramètres entiers

infiniment grands interviennent, et la Géométrie Euclidienne ne pose pas vraiment de difficulté.

Par contre la Géométrie Discrète Arithmétique, cousine de la Géométrie Discrète chargée de décrire les objets évoqués plus haut, et ses relations avec la Géométrie Discrète Idéale sont des sujets qui méritent à notre avis d'être approfondis. Ils combinent effectivement mathématiques classiques et non standard. L'existence d'une théorie discrète idéale est en effet un point d'appui précieux; on pourra y amener une notion discrète, candidate à jouer un rôle de d'alias continu et décider, au vu de ses propriétés limite détectables à partir de là, si elle convient ou non. Remarquons simplement que si nous n'allons pas assez loin, si nous ne franchissons pas la barrière des entiers standard, la notion ne nous éclairera pas facilement sur son comportement dans le monde continu. Une autre remarque heuristique va compléter la description de ces relations. Si les propriétés des objets de la Géométrie Discrète Arithmétique sont à priori complexes, elles ne le sont en général plus après transport dans le territoire euclidien, (cette simplicité est l'une des raisons du choix de la Géométrie comme test des Théories Discrètes Idéales). Nous pouvons espérer, si la Géométrie est bien une famille **continue**, détecter et mieux traiter les points de transition entre le facile et le difficile et utiliser ce mécanisme "d'aller-retour" pour dégager les premières propriétés de la Géométrie Discrète Arithmétique; malgré un comportement parfois déroutant, elle montre beaucoup d'analogies avec sa soeur euclidienne.

Bien que nous ne fournissions dans cette partie que les premiers éléments de cette géométrie: les droites, ils indiquent déjà, conjointement à d'autres, qu'une théorie organisée existe bel et bien. La rencontre d'autant d'acteurs essentiels de Géométrie des Nombres ne peut pas être fortuite. La question qui vient à l'esprit est alors "pourquoi pas plus tôt ?". D'autant que des indices de démarches dans ce sens existent. Nous avons cités ceux qui relèvent de préoccupations dites **algorithmiques**. Or la Géométrie Discrète désigne déjà un domaine mathématique: l'étude des empilements maximaux et des recouvrements minimaux de parties identiques dans un domaine donné. Cette définition de la Géométrie Discrète est entièrement différente de la notre qui est une mathématisation de l'approche algorithmique. Si ce domaine demandait encore à émerger c'est du, selon nous, à l'absence d'une liaison théorique entre cette Géométrie et la Géométrie Euclidienne; il est difficile de progresser sur ce terrain sans l'aide apportée par les outils dérivant du continu.

L'approche concrète, pragmatique, via les nombres, les discrétisations,

l'ordinateur, ont également fait surgir de nombreux indices de son existence et même des vœux pour sa création; mais là aussi un écueil de taille gêne la navigation: les nombres réels et la croyance qu'ils sont indispensables aux fondements des théories continues. Or celles-ci, dès qu'elles sont discrétisées, composées avec l'opérateur de troncature, se comportent de façon radicalement différente, et deviennent quasiment irrécupérables par les méthodes réelles; l'arithmétique réapparaît inévitablement. Même abordé par le côté pratique c'est la modélisation des réels par le choix d'entiers infiniment grands, encore I.S.T., qui a montré qu'il est possible de construire le continu sur un substrat entièrement discret dans lequel la discrétisation est une simple restriction qui ne fait plus intervenir de perturbation.

#### Commentaires

La Géométrie Discrète est une partie de la Géométrie de Nombres, celle qui est concernée par les applications algorithmiques. Certains pourraient être choqués que l'on puisse qualifier de géométriques des structures aussi irrégulières. Nous voyons surtout dans les espaces discrets le moyen d'associer aux fonctions arithmétiques quotient et reste euclidiens un concept "visuel" analogue à celui que les droites, plans ... apportent à la linéarité.

Malgré cette ressemblance cherchée avec les théories réelles cette géométrie a une personnalité assez distincte. Par exemple il est facile d'associer, à chaque droite discrète son "réseau des restes", sous-groupe de  $\mathbb{Z}^2$ , qui en est une sorte de grossissement sur lequel il est plus facile de voir certaines propriétés. Mais les transformées des droites discrètes par des matrices à coefficients entiers font également apparaître des réseaux entiers; par conséquent tout ce que nous savons sur les droites de propage aux restes qui nous font mieux comprendre les droites, redonnant de meilleurs renseignements sur les restes etc.... Bien que les résultats obtenus par cette voie soient tous "équivalents" à des déductions formelles sur les fonctions quotient et reste, leur interprétation géométrique s'avère infiniment plus commode; elle réclame toutefois de dessiner effectivement. Cette théorie donne alors un moyen de d'étudier et de rapprocher de nombreuses questions importantes d'arithmétique.

Comme cela se produit souvent, l'introduction d'objets souhaités dans une théorie s'accompagne d'effets non prévus. Nous avons été surpris de voir avec quelle facilité des objets "fractals" surgissent dans cette géométrie. Comme nous acceptons des objets quasi-linéaires, nombreux sont ceux qui ont des propriétés d'autosimilarité. Cette théorie permet d'aborder "géométriquement"

l'étude de certains fractals. Des expérimentations de P. Nehlig et des travaux en cours de M.A. Jacob et L.L. Hai confirment ce point de vue. Quelques autres résultats montrent que cette Géométrie doit également intervenir dans l'étude de l'Analyse Matricielle en précision limitée (virgule fixe) et permettre de relier la dynamique des processus itératifs discrets ainsi obtenus aux propriétés arithmétiques des coefficients.

LES DROITES DISCRETES

## I UNE NOTION GENERALE DE DROITE DISCRETE

1 La position du problème.

Les droites discrètes ont été abordées de bien des façons, dans le monde des applications, depuis le parcours incrémental des points entiers les plus voisins d'une droite rationnelle de Bresenham [10], jusqu'aux petits harpons de Greene-Yao [48] en passant par l'étude des propriétés intrinsèques des discrétisations d'une droite de Freeman [46] et Pham [80] et [82]. En effet la droite de meilleure approximation entière n'est pas la seule façon de discrétiser une droite rationnelle de pente  $\frac{a}{b}$ . Comme pour un nombre réel qui peut, dans une arithmétique à virgule fixe, être remplacé par le nombre décimal le plus voisin ou par le nombre décimal tronqué, une droite réelle peut être approchée par la droite de meilleure approximation entière (droite de Bresenham) ou par la droite discrète, que nous qualifions de naïve, constituée par l'ensemble des points  $(i, \left[ \frac{ai}{b} \right])$  de  $\mathbb{Z}^2$  lorsque  $i \in \mathbb{Z}$ ,  $[\ ]$  étant la partie entière; cette dernière pourrait aussi être qualifiée de droite des troncatures; (notre qualificatif naïf sera précisé et justifié plus loin).

Toutes les approches antérieures de la notion de droite discrète pèchent par l'emploi de concepts continus, en particulier de nombres réels, source de maintes difficultés. Conformément à la philosophie développée dans l'introduction générale nous arithmétisons la situation le plus rapidement possible. Plus précisément nous introduisons certains sous-ensembles de  $\mathbb{Z}^2$  arithmétiquement paramétrés qui englobent toutes les notions de droites discrètes utilisées jusque là en Traitement de l'image, Informatique Graphique et Géométrie Algorithmique. La traduction, dans notre contexte, des questions posées par l'utilisation pratique des droites discrètes permet, en utilisant les outils classiques de l'arithmétique (inéquations Diophantiennes, réseaux, dénombrement de points de réseaux, fractions continues...) de leur apporter des réponses simples et de fournir de nouveaux algorithmes. Ainsi nous résolvons le problème de la détermination de l'intersection de deux droites discrètes en donnant, pour cette intersection, d'une part un algorithme de paramétrage et d'autre part les conditions nécessaires et suffisantes sur leurs paramètres pour sa connexité ou non-connexité.

## 2 Définition diophantienne des droites discrètes.

### Définition 1

Une droite discrète est l'ensemble des points entiers d'une bande plane; autrement dit c'est l'ensemble  $\mathcal{D}$  des points  $(x,y)$  de  $\mathbb{Z}^2$  vérifiant deux inégalités:

$$\gamma \leq ax+by < \gamma' \quad (\mathcal{D})$$

où  $a,b,\gamma,\gamma'$  sont réels,  $a$  et  $b$  premiers entre eux.

Une droite discrète **rationnelle**  $\mathcal{D}$  est une droite discrète où les paramètres  $a,b$ , sont entiers et  $\gamma,\gamma'$  réels. Dans le cas où  $\gamma$  et  $\gamma'$  ne sont pas entiers l'ensemble des couples  $(x,y)$  tels que  $(x,y) \in \mathbb{Z}^2$  et  $\gamma \leq ax+by \leq \gamma'$  est identique à l'ensemble  $\{(x,y) \mid (x,y) \in \mathbb{Z}^2 \text{ et } [\gamma]+1 \leq ax+by \leq [\gamma']\}$  où  $[ ]$  désigne la partie entière; nous pouvons donc toujours supposer  $\gamma$  et  $\gamma'$  entiers dans la définition d'une droite discrète. Dans la suite nous ne nous intéressons qu'aux droites discrètes rationnelles.

- o Le vecteur  $(a,b)$  est le **vecteur normal** de la droite,
- o les entiers  $\gamma$  et  $\gamma'$  sont les **bornes** de la droite et
- o l'entier  $\omega = \gamma' - \gamma$  est l'**épaisseur arithmétique** de la droite.

Nous appellerons **pointillé** l'ensemble des solutions d'une équation diophantienne

$$ax+by=v.$$

et le désignerons généralement par  $\pi(a,b)(v)$ , ou  $\pi(v)$  lorsque le vecteur normal est sous-entendu. Nous dirons aussi que deux pointillés associés à la même équation  $ax+by$  et à des second membres  $v$  et  $v+1$  sont **consécutifs**. Une droite discrète est donc constituée de la réunion de pointillés consécutifs, l'épaisseur étant le nombre de ceux-ci.

Nous désignerons par

$$\mathcal{D}(a,b,\gamma,\omega) \quad (1)$$

la droite définie par les inéquations

$$\gamma \leq ax+by < \gamma+\omega \quad (\mathcal{D})$$

En utilisant la structure bien connues des solutions de l'équation diophantienne linéaire

$$ax+by=v$$

où  $a,b,v \in \mathbb{Z}$ , cette décomposition de  $\mathcal{D}$  nous permet d'accéder à ses points.

La **structure** d'une droite discrète est la succession de ses paliers.

Bien que celle-ci soit descriptible par la décomposition diophantienne précédente, le nombre de calculs nécessaires à la résolution directe de ces équations pour  $v \in [\gamma, \gamma + \omega[$  rend à priori la notion de droite discrète inutilisable en algorithmique. Elle ne l'est pas plus en théorie: les formules qui définissent les points de  $(\mathcal{D})$  ne pouvant pas être utilisées directement pour analyser ses structures. L'enjeu va consister essentiellement à les dégager peu à peu de la définition introduite en suivant un chemin qui soit le plus proche possible du terrain algorithmique.

Pour étudier les relations entre les aspects analytiques et géométriques des droites discrètes introduisons l'équation d'une droite discrète:  $(\mathcal{D})$  est aussi l'ensemble

$$(\mathcal{D}) = \{(x, y) \mid \left[ \frac{ax+by-\gamma}{\omega} \right] = 0\}$$

où  $\left[ \frac{\alpha}{\beta} \right]$  désigne le quotient de la division euclidienne de  $\alpha$  par  $\beta$  (ou la partie entière du rationnel  $\frac{\alpha}{\beta}$ ).

Mais il existe de nombreuses manières de représenter  $(\mathcal{D})$  par une telle expression. Soit  $(x_0, y_0)$  une solution de l'équation diophantienne  $ax+by=\gamma$ , la droite  $\mathcal{D}$  est également l'ensemble

$$(\mathcal{D}) = \{(x, y) \mid \left[ \frac{a(x-x_0)+b(y-y_0)}{\omega} \right] = 0\}$$

Plus généralement si  $(x_0, y_0)$  est une solution de l'équation diophantienne  $ax+by=\gamma+\varepsilon$  où  $\varepsilon \in [0, \omega[$ , donc un point quelconque de  $(\mathcal{D})$  nous avons

proposition 1 ( Equations d'une droite discrète )

*La droite discrète  $(\mathcal{D})$  coïncide avec l'ensemble défini par l'équation:*

$$(\mathcal{D}) = \{(x, y) \mid \left[ \frac{a(x-x_0)+b(y-y_0)+\varepsilon}{\omega} \right] = 0\} \quad (2)$$

Nous dirons que  $\mathcal{D}$  a pour  **pente**   $\frac{a}{b}$ , passe par  $(x_0, y_0)$ , a pour épaisseur  $\omega$  et possède en  $(x_0, y_0)$  un  **reste**  égal à  $\varepsilon$ ; lorsque une droite discrète  $\mathcal{D}$  est définie par l'une de ses équations précédentes. La notion d'équation d'une droite n'est plus intrinsèque comme elle l'est en Géométrie Euclidienne. C'est la notation (1) qui s'avère la plus commode pour représenter une droite discrète.

### 3 Droites discrètes équivalentes.

Abordons quelques questions d'invariance concernant ces droites discrètes. Désignons, pour tout sous-ensemble  $X$  de  $\mathbb{Z}^2$  et tout vecteur entier

$\tau=(s,t)$ , par  $\tau+X$  le translaté de  $X$  de vecteur  $\tau$  i.e. l'ensemble  $\{\tau+x|x\in X\}$ . Nous dirons que deux droites discrètes  $\mathcal{D}$  et  $\mathcal{D}'$  sont **équivalentes** si et seulement s'il existe un vecteur de translation entier  $\tau=(s,t)$  tel que  $\mathcal{D}'=\tau+\mathcal{D}$ .

théorème 1 (premier théorème de structure)

Si  $a$  et  $b$  (resp.  $a'$  et  $b'$ ), sont premiers entre eux les droites  $\mathcal{D}(a,b,\gamma,\omega)$  et  $\mathcal{D}'(a',b',\gamma',\omega')$  sont équivalentes si et seulement si l'on a  $a=a'$ ,  $b=b'$  et  $\omega=\omega'$ .

Cette propriété se déduit immédiatement du fait suivant: si  $\pi(c)$  et  $\pi(c')$  sont les pointillés de bornes respectives  $c$  et  $c'$  et si le vecteur entier  $\tau$  vérifie  $\tau + \pi(c) = \pi(c')$  alors on a  $\tau + \pi(c+1) = \pi(c'+1)$ .

Il est clair que la droite  $\mathcal{D}(a,b,\gamma,\omega)$  est invariante par les translations de vecteurs  $k(b,-a)$ , où  $k\in\mathbb{Z}$ . De plus, si  $|a|<|b|$  et si  $x_0\in\mathbb{Z}$  est donné, chaque pointillé de  $\mathcal{D}$  contient un et un seul point d'abscisse  $x\in[x_0, x_0+|b|[$ . Nous appellerons **période** de  $\mathcal{D}$  l'ensemble de ses points dont les abscisses appartiennent à un tel intervalle de longueur  $|b|$ . Le plus souvent nous prendrons  $x_0=0$ .

#### 4 Le rôle du reste d'une droite discrète. Le calcul modulaire.

Le passage de  $\varepsilon$  à  $\varepsilon+\delta$  dans l'équation (2) provoque, en introduisant une solution  $x_1,y_1$  de l'équation  $ax_1+by_1=\delta$ , une modification du **point initial**. La droite perturbée, d'équation

$$\left[ \frac{a(x-x_0)+b(y-y_0)+\varepsilon+\delta}{\omega} \right] = 0,$$

a aussi pour équation

$$\left[ \frac{a(x-x_0+x_1)+b(y-y_0+y_1)+\varepsilon}{\omega} \right] = 0.$$

Le changement du reste d'une droite discrète provoque simplement une translation de celle-ci.

Le rôle du reste se voit également très bien dans l'expression du vecteur de translation entre  $\pi(c)$  et  $\pi(c+1)$ :

Si  $u$  et  $v$  sont les coefficients de Bezout de  $a$  et  $b$ , i.e. tels que l'on ait:

$$au + bv = 1$$

alors les vecteurs de translation  $\tau$  tels que  $\tau + \pi(c) = \pi(c+1)$  sont de la forme  $(u,v) + k(b,-a)$  où  $k\in\mathbb{Z}$ . Or nous pouvons prendre  $u \equiv a^{-1} \pmod{b}$  et par conséquent les pointillés consécutifs  $\pi(c)$ ,  $\pi(c+1)$ ,  $\pi(c+2)$ , ..,  $\pi(c+k)$ , .. sont

positionnés par le vecteur  $(ku \text{ mod } b, kv \text{ mod } a)$  à partir d'un point de  $\pi(c)$ .

Ce reste joue un rôle comparable à celui de la condition initiale d'une solution d'équation différentielle. Ici une perturbation minimale,  $\delta=1$ , provoque une translation de la droite; mais comme cette translation s'effectue parallèlement à celle-ci elle ne provoque que peu de modifications. Il est facile de constater que cette modification supprime l'un des pointillés qui la borde et lui en accole un sur son bord opposé.

La considération de la décomposition diophantienne des droites discrètes élargit le cadre des objets ainsi désignés jusque là. Cet enrichissement, qui permet de mieux comprendre leurs liens avec les droites euclidiennes, pose par contre le problème d'étendre les théorèmes de structure et les algorithmes déjà connus pour ces dernières. Pour y parvenir nous suivrons pas à pas l'effet du reste  $\varepsilon$ , ce qui nous conduira à décrire la structure d'une droite discrète par voie **modulaire**, ie par la suite  $a_i$  modulo  $b$ , notée plus loin  $\left\{ \frac{a_i}{b} \right\}$ .

## 5 Topologie des droites discrètes:

### Droites 8-connexes, 4-connexes et \*-connexes.

Les notions bien connues dans la pratique de courbes discrètes 4 ou 8-connexes définissent sur  $\mathbb{Z}^2$  deux topologies (non séparées) analogues à la topologie usuelle du plan continu  $\mathbb{R}^2$ . Le type "topologique" d'une droite discrète peut être caractérisé arithmétiquement. Nous avons

#### proposition 3

*La droite  $\mathcal{D}(a,b,\gamma,\omega)$  est 8-connexe ssi  $\omega \geq \sup(|a|, |b|)$ ; elle est 4-connexe ssi  $\omega \geq |a| + |b|$ .*

Si  $0 \leq |a| \leq |b|$  et si  $\mathcal{D}$  est 8-connexe elle possède au moins  $b$  points dans sa période (d'abscisses  $\in [0, b[$ ). Or chaque pointillé ne possède qu'un point par période, donc  $|b|$  pointillés au moins sont requis, d'où  $\omega \geq |b|$ . Réciproquement si  $\omega \geq |b|$  la droite contient la suite de points  $(x, \left[ \frac{\gamma - ax}{b} \right])$  qui est 8-connexe. Idem pour la 4-connexité, le paramétrage requis des droites 4-connexes sera donné au §III suivant.

Nous qualifions de **naïve** toute droite discrète  $\mathcal{D}(a,b,\gamma,\omega)$  pour laquelle  $\omega = \sup(|a|, |b|)$ .

## Définition 2

Nous dirons que la droite  $\mathcal{D}(a,b,\gamma,\omega)$  est  $*$ -connexe si et seulement si  $\omega$  vérifie la double inégalité  $\sup(|a|,|b|) < \omega < |a|+|b|$ .

L'approche arithmétique possède l'avantage de pouvoir contrôler la **topologie** des droites discrètes avec un seul paramètre, l'épaisseur  $\omega$ , depuis le cas des pointillés ( $\omega=1$ ) jusqu'aux droites 4-connexes en passant par les droites  $*$ -connexes et nous invitant à aller voir au-delà, vers les droites **épaisses** ( $\omega > |a|+|b|$ ). Remarquons que ce sont les droites  $*$ -connexes qui ont un caractère **générique**, une droite épaisse étant généralement réunion d'un nombre entier de droites naïves et d'une droite  $*$ -connexe.

## 6 Relation avec les notions antérieures.

Montrons que notre définition contient les diverses notions de droites discrètes déjà introduites dans la littérature spécialisée.

Digitalisation d'une droite réelle de pente rationnelle.

Considérons la droite réelle de pente rationnelle  $D$  d'équation  $ax+by+c=0$  où  $a,b,c \in \mathbb{Z}$ , dans [41] est introduit, sous le vocable de "digitalisation de  $D$ ", l'ensemble des points entiers appartenant à  $D$ . Nous constatons que c'est exactement l'ensemble des solutions de l'équation diophantienne  $ax+by+c=0$ . Si nous désignons par  $(x_0, y_0)$  une solution quelconque de cette équation cette digitalisation n'est autre que  $\mathcal{D}(a,b,-c,1)$ .

Droite discrète par défaut, par excès et de meilleure approximation.

Soit  $D$  une droite réelle de pente rationnelle d'équation  $ax+by+c=0$  avec  $a,b,c \in \mathbb{Z}$ . Considérons, en supposant  $b=|b|=\sup(|a|,|b|)$ , l'ensemble des points entiers  $\{(x,y) | y = \left[ \frac{-ax-c}{b} \right]\}$ ; il est identique à l'ensemble des points entiers  $(x,y)$  vérifiant  $-b-c+1 \leq ax+by < -c+1$  c'est à dire à la droite discrète  $\mathcal{D}(a,b,-b-c+1,b)$ . C'est la droite discrète par défaut associée à  $D$ .

De même la droite discrète par excès associée à  $D$  coïncide avec la droite  $\mathcal{D}(a,b,-c+1,b)$ .

La droite des points de meilleure approximation entière, ou droite de Bresenham associée à la droite réelle  $D$  ci-dessus est formée des points entiers les plus voisins. Désignons par  $d((x,y),D)$  la distance euclidienne d'un point  $(x,y)$  du plan à  $D$ . Pour tout point  $x_0$  de  $\mathbb{Z}$  la fonction  $\text{Inf } d((x_0,y),D)$  est bien définie et est atteinte en un point  $y_0$  en général  $y_0 \in \mathbb{Z}$  unique (ou en deux points au plus situés de part et d'autre de  $D$ ). Toujours sous l'hypothèse  $b=|b|=\sup(|a|,|b|)$  il est facile de montrer qu'elle coïncide avec  $\mathcal{D}(a,b,-c+1-\lfloor \frac{b}{2} \rfloor, b)$ .

Droite discrète recouvrante.

C'est la droite formée par les pixels traversés par une droite réelle  $D$  de pente rationnelle et d'équation  $ax+by+c=0$ ; plus précisément nous distinguons deux notions de droite recouvrante, la droite recouvrante stricte et la droite recouvrante large. Le pixel de coordonnées entières  $(x_0, y_0)$  est le sous-ensemble de  $\mathbb{R}^2$  formé des points  $(x, y)$  définis par

$$\{(x, y) \mid (x, y) \in \mathbb{R}^2 \text{ et } \sup(|x-x_0|, |y-y_0|) < 1\}$$

Nous dirons que  $D$  traverse strictement le pixel  $(x_0, y_0)$  si  $D$  rencontre son intérieur, c'est à dire s'il existe un point  $(x, y) \in D$  tel que  $0 < \sup(|x-x_0|, |y-y_0|) < 1$  et que  $D$  traverse ce pixel au sens large si  $D$  passe par  $(x_0, y_0)$  mais ne contient que des points frontière de  $D$ . La notion de droite discrète recouvrante au sens strict est constituée des pixels que  $D$  coupe strictement, la deuxième accepte aussi les pixels intersectés au sens large. Il est alors facile de vérifier la

proposition 4

*Soit  $D$  la droite réelle de pente rationnelle et d'équation  $ax+by+c=0$ , où  $a, b, c \in \mathbb{Z}$ , et  $0 \leq a \leq b$  alors*

*a) La droite de recouvrement au sens large de  $D$  a pour épaisseur  $\omega = a+b$ , i.e. elle est 4-connexe*

*b) La droite de recouvrement au sens strict a pour épaisseur  $\omega = a+b-1$  (elle est \*-connexe).*

*Dans les deux cas la droite de recouvrement est la droite discrète:*

$$\mathcal{D}(a, b, -a-c, \omega).$$

Il résulte du premier théorème de structure que si  $D$  est une droite réelle donnée, comme ci-dessus, les droites par défaut, par excès et de meilleure approximation entière (de Bresenham) sont **équivalentes**, i.e. coïncident à translation près. Plus généralement toutes les droites naïves de vecteur normal  $(a, b)$  fixé sont équivalentes.

7 Symétries des droites discrètes.

Les droites discrètes possèdent des symétries intéressantes qui permettent de restreindre leur étude au cas  $0 \leq a < b$ . Soit  $\mathcal{D}(a, b, \gamma, \omega)$  une droite discrète, alors la transformée par la symétrie par rapport

- o à  $Ox$  est  $\mathcal{D}(a, -b, \gamma, \omega)$ ,
- o à  $Oy$  EST  $\mathcal{D}(-a, b, \gamma, \omega)$ ,
- o à  $O$  EST  $\mathcal{D}(-a, -b, \gamma, \omega)$  OU  $\mathcal{D}(a, b, -\gamma - \omega + 1, \omega)$ ,
- o à la droite  $X = x_0$ ,  $x_0 \in \mathbb{Z}$ , est  $\mathcal{D}(-a, b, \gamma - 2ax_0, \omega)$
- o à la droite  $Y = y_0$ ,  $y_0 \in \mathbb{Z}$ , est  $\mathcal{D}(a, -b, \gamma - 2by_0, \omega)$

o à la première bissectrice est  $\mathcal{D}(b,a,\gamma,\omega)$

o au point  $(x_0, y_0)$  est  $\mathcal{D}(-a, -b, \gamma - 2(ax_0 + by_0), \omega) =$   
 $\mathcal{D}(a, b, -\gamma + 2(ax_0 + by_0) - \omega + 1, \omega)$ .

La droite  $\mathcal{D}(a,b,\gamma,\omega)$  contient des points de symétrie ssi son épaisseur  $\omega$  est impaire  $\omega=2\nu+1$ ; dans ce cas ses points de symétrie sont ceux du pointillé central  $\pi(\gamma+\nu)$ .

Remarque: ces symétries ne sont pas les seules; des symétries **rationnelles** existent par rapport aux centres des pixels. Elles suffisent néanmoins pour réduire l'étude des structures aux droites passant par l'origine et contenues dans le premier octant i.e. vérifiant  $0 \leq a \leq b$ , et  $(a,b)=1$ .

## II DROITES DISCRETES ET GROUPE MODULAIRE.

### 1 Droites discrètes homologues.

Nous avons déjà vu que deux droites discrètes sont *équivalentes* (i.e. égales à translation près) ssi elles ont même pente et même épaisseur. Nous cherchons ce qui, dans la structure d'une droite discrète, dépend plus précisément:

- o des bornes,
- o de l'épaisseur  $\omega$ ,
- o du paramètre de pente (i.e. du vecteur entier  $(a,b)$ ).

#### Définition 1

Nous dirons que deux droites discrètes  $\mathcal{D}$  et  $\mathcal{D}'$  sont **HOMOLOGUES** ssi il existe une matrice  $M$  de  $Sl(2,\mathbb{Z})$ , (i.e. matrice  $2 \times 2$  à coefficients entiers et de déterminant 1) telle que  $\mathcal{D}' = M\mathcal{D}$ .

#### Théorème 1 (deuxième théorème de structure)

Deux droites discrètes sont **HOMOLOGUES** ssi elles ont les mêmes bornes.

démonstration

L'action de  $Sl(2,\mathbb{Z})$  sur  $\mathbb{Z}^2$  peut s'écrire  $M \begin{pmatrix} a \\ b \end{pmatrix}$  ou  $(a,b)M^t$ , où  $M^t$  est la transposée de  $M$ . Considérons la droite  $\mathcal{D}(a,b,\gamma,\omega)$  d'inéquations:

$$\gamma \leq ax+by < \gamma+\omega$$

qui peuvent se réécrire:

$$\gamma \leq (a \ b) \begin{pmatrix} x \\ y \end{pmatrix} < \gamma+\omega$$

ou encore

$$\gamma \leq (a \ b) M^{-1} \cdot M \begin{pmatrix} x \\ y \end{pmatrix} < \gamma+\omega.$$

Cette dernière relation montre que

$$M \cdot \mathcal{D}(a,b,\gamma,\omega) = \mathcal{D}((a,b)M^{-1},\gamma,\omega)$$

ou  $\mathcal{D}(a',b',\gamma,\omega)$  si l'on pose  $(a',b')=(a,b)M^{-1}$ .

Montrons, réciproquement, que deux droites  $\mathcal{D}(a,b,\gamma,\omega)$  et  $\mathcal{D}(a',b',\gamma,\omega)$  ayant les mêmes bornes  $\gamma$  et  $\gamma+\omega$  se correspondent par une transformation unimodulaire i.e. sont **homologues**.

S'il existe un opérateur unimodulaire  $M$  tel que  $(a',b')M = (a,b)$  alors les inéquations de  $\mathcal{D}'$  s'écrivent:

$$\gamma \leq (a' \ b')M.M^{-1} \begin{pmatrix} x \\ y \end{pmatrix} < \gamma + \omega$$

soit encore

$$\gamma \leq (a \ b) \begin{pmatrix} X \\ Y \end{pmatrix} < \gamma + \omega$$

où  $\begin{pmatrix} X \\ Y \end{pmatrix} = M^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$ ; ceci signifie que  $M^{-1}\mathcal{D}'$  est contenue dans la droite  $\mathcal{D}$ . Comme  $M$  est inversible, un calcul analogue montre que  $M\mathcal{D} \subseteq \mathcal{D}'$ ; d'où l'égalité  $M\mathcal{D} = \mathcal{D}'$ .

Déterminons  $M$  tel que  $(a' \ b')M = (a \ b)$ . Posons  $M = \begin{pmatrix} m & p \\ n & q \end{pmatrix}$ , où  $m, n, p, q \in \mathbb{Z}$  et  $mq - np = 1$ . La condition s'écrit

$$\begin{cases} ma' + nb' = a \\ pa' + qb' = b \end{cases}$$

Soit  $(m_0, n_0)$  une solution de  $ma' + nb' = 1$ , alors toutes les solutions du système précédent sont données par la matrice paramétrée suivante:

$$\begin{pmatrix} m_0 a + kb' & m_0 b + lb' \\ n_0 a - ka' & n_0 b - la' \end{pmatrix}, \quad k \text{ et } l \in \mathbb{Z}.$$

Son déterminant étant égal à 1, nous avons la relation:

$$(m_0 a' + n_0 b')(-la + kb) = 1$$

qui, d'après la définition de  $(m_0, n_0)$ , se réduit à

$$kb - la = 1.$$

Si  $(k, l)$  est une solution de cette équation diophantienne il lui correspondra un opérateur unimodulaire  $M$ .

### Exemple

Les droites  $\mathcal{D}(-5, 17, 11, 26)$  et  $\mathcal{D}(9, 4, 11, 26)$  sont homologues; écrire la transformation unimodulaire qui fait passer de l'une à l'autre.

On résoud l'équation

$$(-5, 17) M = (9 \ 4),$$

qui donne

$$M = \begin{pmatrix} 56 & 23 \\ 17 & 7 \end{pmatrix}.$$

### Corollaire 1

Deux droites discrètes sont en **bijection** (affine) ssi elles ont la même épaisseur.

C'est clair: si les deux droites ont les mêmes épaisseurs on peut, en translatant l'une d'elles, se ramener au cas où elles ont les mêmes bornes.

## 2 Paliers et groupe modulaire.

Le groupe modulaire décrivant toutes les droites *TOURNANT AUTOUR DE DEUX BORNES*, permet également de décrire, indépendamment du calcul modulaire, la structure en paliers de chacune d'elles.

Montrons que la décomposition d'un opérateur unimodulaire en produit de **transvections élémentaires** de matrices

$$L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ ET } U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix};$$

traduit la structure en paliers liée à la pente d'un droite discrète.

Les paliers généralisés.

Les paliers horizontaux (resp. verticaux) de  $\mathcal{D}(a, b, \gamma, \omega)$  sont les segments formés par l'intersection de  $\mathcal{D}$  avec une droite horizontale d'équation  $y=k$ , (resp. verticale d'équation  $x=k$ ), où  $k \in \mathbb{Z}$ .

Les **longueurs des paliers horizontaux** sont les deux entiers consécutifs

$$\left[ \frac{\omega}{a} \right] \text{ et } \left[ \frac{\omega}{a} \right] + 1 \text{ si } \left\{ \frac{\omega}{a} \right\} \neq 0$$

et l'entier

$$\left[ \frac{\omega}{a} \right] \text{ SI } a \text{ DIVISE } \omega.$$

De même les **longueurs des paliers verticaux** sont les entiers consécutifs

$$\left[ \frac{\omega}{b} \right] \text{ et } \left[ \frac{\omega}{b} \right] + 1 \text{ SI } \left\{ \frac{\omega}{b} \right\} \neq 0$$

et l'entier

$$\left[ \frac{\omega}{b} \right] \text{ SI } b \text{ DIVISE } \omega.$$

Supposons  $a$  et  $b$  premiers entre eux et  $|a| < |b|$  et désignons par  $\ell = \left[ \frac{b}{a} \right]$  la longueur des paliers horizontaux courts de la droite naïve  $\delta$  d'inéquations

$$\gamma \leq ax + by < \gamma + |b|$$

qui **borde** la droite  $\mathcal{D}$ ; ses paliers verticaux sont tous de longueur 1.

L'opérateur  $M_\ell = \begin{pmatrix} 1 & \ell \\ 0 & 1 \end{pmatrix}$  applique  $\mathcal{D}(a, b, \gamma, \omega)$  sur la droite  $\mathcal{D}'$  définie par

$$\gamma \leq ax + (b - \ell a)y < \gamma + \omega$$

mais la division euclidienne de  $b$  par  $a$  donne l'égalité  $b = \ell a + r$  où  $r \in [0, a[$ ; la droite  $\mathcal{D}'$  est donc définie par

$$\gamma \leq ax + ry < \gamma + \omega$$

donc la **transvection géométrique**  $M_\ell$ , qui **efface les paliers courts** du bord de la droite  $\mathcal{D}$ , opère simultanément une étape de l'**Algorithme d'Euclide** sur le vecteur pente  $(a, b)$ .

En itérant ce processus jusqu'à ce qu'une composante de la pente soit

égale à 1 et l'autre à 0 on obtient une matrice unimodulaire  $M$ , produit des opérateurs  $M_\ell$  ainsi obtenus, canoniquement associée à  $\mathcal{D}$ . Elle applique  $\mathcal{D}$  bijectivement sur une bande horizontale (ou verticale) de  $\mathbb{Z}^2$ , d'épaisseur  $\omega$ .

Nous retrouvons le théorème 1 précédent sous une forme équivalente, géométrique, disant que les droites discrètes sont homologues à une bande verticale:

### Théorème 2

*La droite discrète  $\mathcal{D}(a, b, \gamma, \omega)$  est égale à  $M \cdot \Delta(1, 0, \gamma, \omega)$  où  $M = \begin{pmatrix} u & -b \\ v & a \end{pmatrix}$  est unimodulaire et  $au + bv = 1$ .*

Par conséquent l'ensemble de toutes les droites discrètes s'identifie au produit:

$$\mathbb{Z} \times \mathbb{N} \times \text{Sl}(2, \mathbb{Z})$$

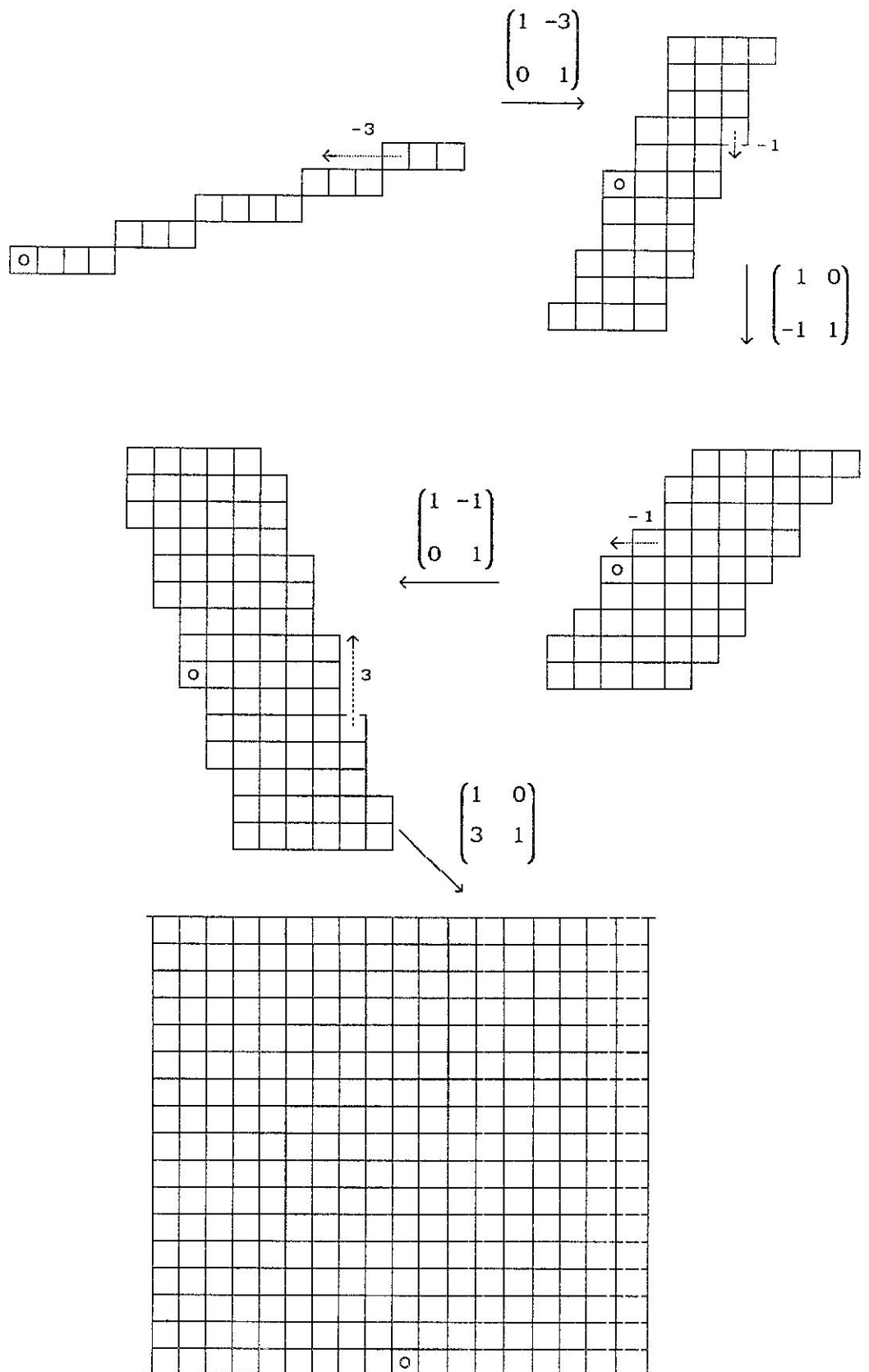
par la correspondance: (**borne inférieure, épaisseur, pente**).

Remarque: il est possible de donner un sens algébrique à l'épaisseur afin de ramener l'ensemble des droites discrètes au groupe  $\mathbb{Z} \times \mathbb{Z} \times \text{Sl}(2, \mathbb{Z})$ .

Si l'on veut amener la bande verticale  $\Delta$  précédente sur  $\mathcal{D}$  par des transvections horizontales et verticales, ce qui est particulièrement bien adaptée aux architectures des mémoires et des cartes graphiques, il suffit de décomposer l'opérateur  $M$  en produit de  $L$  et  $U$ . La décomposition est donnée par les quotients partiels du développement en fraction continue de la pente  $\frac{a}{b}$ .

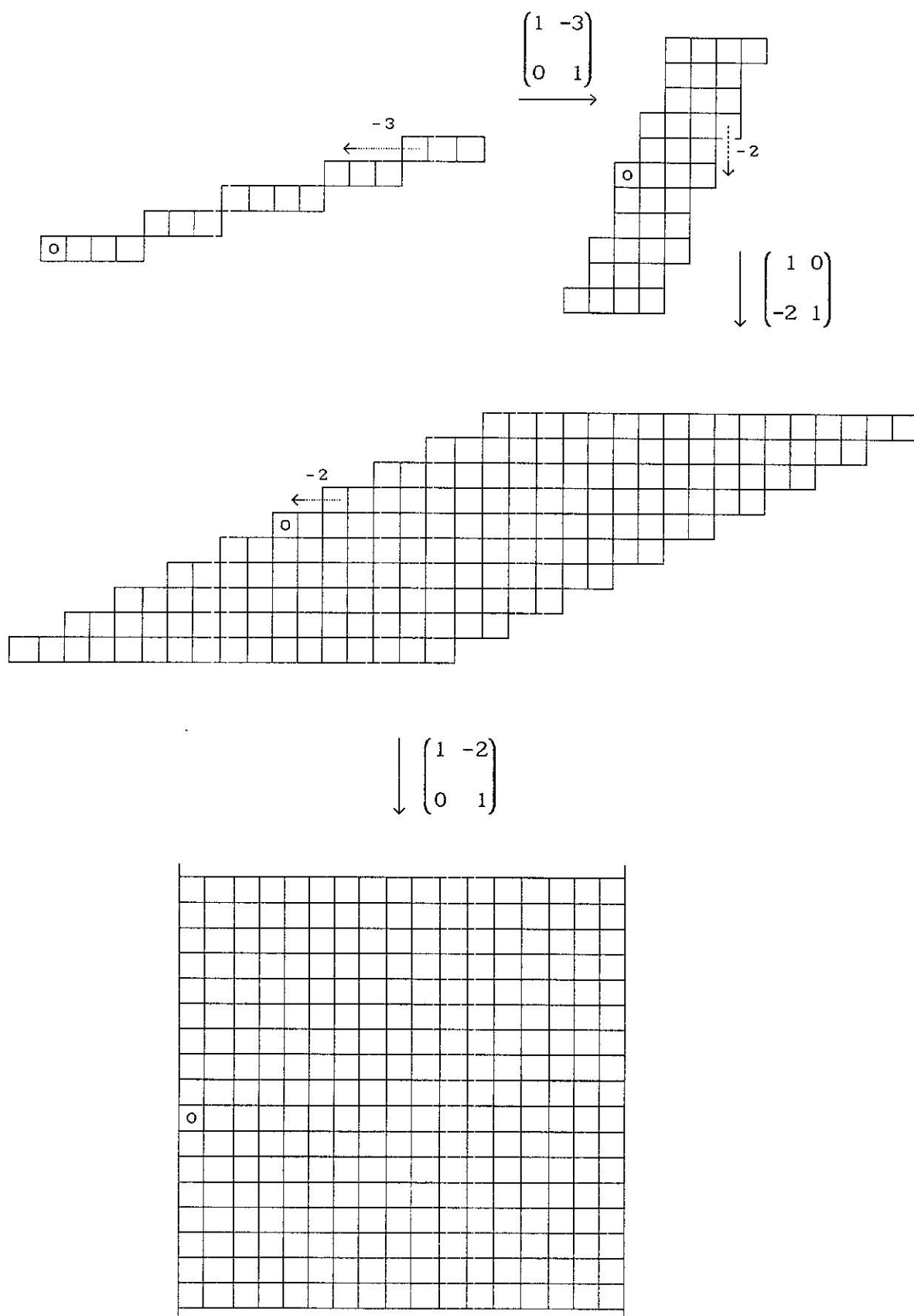
Exemple

La figure suivante représente une suite de transvections qui ramènent  $\mathcal{D}(5, -17, 0, 17)$  sur la bande horizontale  $0 \leq y < 17$  de même épaisseur.



Exemple

La figure suivante représente la suite des transvections canoniques de  $\mathcal{D}(5, -17, 0, 17)$  (modules égaux aux longueurs des petits paliers). La droite est appliquée sur la bande  $0 \leq x < 17$ .



Nous utiliserons plusieurs fois ce deuxième théorème de structure. La décomposition en transvections  $L$  et  $U$  est particulièrement bien adaptée aux structures des mémoires et des écrans graphiques dont les déplacements des lignes et des colonnes sont des primitives de base (ces matériels ne sont pas encore les plus répandus aujourd'hui, les déplacements de lignes étant les seuls privilégiés).

Ce résultat permet d'aborder quelques questions intéressantes concernant les droites discrètes: les tracés et parcours. Il n'autorise pas, toutefois, de traiter toutes les questions naturelles que l'on peut se poser à leur sujet: lacunes et composantes connexes. Par compte il met en lumière le rôle prépondérant joué par le groupe unimodulaire et non pas par le développement en fraction continue de la pente  $\frac{a}{b}$ . Ceci permet d'envisager l'étude des objets quasi-linéaires de dimensions quelconques auxquels il conviendrait d'étendre les résultats de ce travail. Nous nous contentons ici d'en donner la définition

Définition 1

Si  $\mathbf{a} \in \mathbb{Z}^{n+1}$  et  $\omega \in \mathbb{N}$  nous appellerons **hyperplan** discret de vecteur normal  $\mathbf{a}$  et d'épaisseur  $\omega$ , l'ensemble des solutions entières des inéquations

$$\rho \leq \mathbf{a} \cdot \mathbf{x} < \rho + \omega$$

où  $\rho \in \mathbb{Z}$ . Plus généralement un **ensemble quasi-linéaire** discret sera constitué par l'intersection d'un nombre fini d'hyperplans discrets.

### III LES PREMIERS ALGORITHMES DE TRACE DES DROITES DISCRETES.

Nous abordons dans ce paragraphe la question des algorithmes de parcours (tous les points sont examinés) et de tracé (les points sont regroupés par segments) des droites discrètes. Le problème posé est celui de la recherche et de l'étude de la complexité de divers processus itératifs de partition (ou pavage), en points ou en blocs, d'une telle droite.

Nous donnons ici les premiers algorithmes, les plus naturels, de performances comparables à l'algorithme le plus utilisé aujourd'hui: celui de Bresenham. Ils serviront de point de départ à notre recherche de variantes plus performantes et préciserons le rôle de la suite des restes déjà abordé en I 4. Ils conduisent naturellement à l'étude de ses propriétés.

#### 1 Le tracé des droites naïves

Revenons momentanément à la droite naïve de pente  $\frac{a}{b}$  passant par l'origine,  $\mathcal{D}(a,-b,0,b)$ , dont l'équation est par conséquent

$$\left[ \frac{ax-by}{b} \right] = 0$$

ses coefficients vérifiant les conditions  $0 < a < b$  et  $(a,b)=1$ , i.e.  $a$  et  $b$  sont premiers entre eux.

L'ensemble des solutions  $(x,y)$  admet un paramétrage de la forme

$$y = \left[ \frac{ax}{b} \right]$$

où  $x \in \mathbb{Z}$ .

Les symétries du I 7 montrent que les hypothèses sur  $a$  et  $b$  ne sont pas une restriction; d'ailleurs ce paramétrage se généralise sans difficulté comme le lecteur peut le vérifier.

Cette droite naïve représente donc une suite arithmétique tronquée par la fonction partie entière. Sa structure révèle des propriétés de cette fonction. Considérons l'égalité de division euclidienne de  $ax$  par  $b$ ; nous avons

$$\frac{ax}{b} = \left[ \frac{ax}{b} \right] + \frac{\left\{ \frac{ax}{b} \right\}}{b}$$

où  $\left\{ \frac{ax}{b} \right\}$  désigne le reste de cette division. Ce reste appartient à l'intervalle  $[0,b[$ . Cette relation montre que la droite naïve est une approximation par défaut de la droite rationnelle  $y = \frac{ax}{b}$  et que l'erreur commise dans cette approximation est proportionnelle,  $b$  étant fixé, au reste  $\left\{ \frac{ax}{b} \right\}$  aussi désigné par  $ax \text{ modulo } b$ . Autrement dit  $\mathcal{D}$  se comporte comme la partie principale d'une droite rationnelle usuelle. Nous allons illustrer dans la suite le principe, à priori paradoxal, que toute l'information sur une droite discrète est contenue, et assez facilement accessible, dans sa suite des restes, i.e. dans

la partie généralement négligée. C'est clair si l'on observe que la quantité d'information est exactement la même dans les deux objets étant donnée par le couple d'entiers (a,b). Les suites  $\left[ \frac{ax}{b} \right]$  et  $\left\{ \frac{ax}{b} \right\}$  ne sont qu'un transcodage l'une de l'autre; dans la suite nous réserverons le terme de suite arithmétique (ou suite des restes) à la deuxième  $\left\{ \frac{ax}{b} \right\}$ .

La première relation qui va nous être utile vient de la remarque suivante: les paliers de la suite  $y_0(x) = \left[ \frac{ax}{b} \right]$  correspondent exactement aux **séquences montantes** de  $y_1(x) = \left\{ \frac{ax}{b} \right\}$ . De plus la dernière étant périodique de période b, la première est pseudo-périodique de période vectorielle (b,a).

Exemple.

Prenons  $\frac{a}{b} = \frac{5}{17}$ , et rassemblons les valeurs d'une période de ces deux suites dans un tableau.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$y_0$	0	0	0	0	1	1	1	2	2	2	2	3	3	3	4	4	4
$y_1$	0	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12

Dans la période suivante,  $x \in [17,33]$ , les valeurs de  $y_0$  sont les précédentes augmentées de 5; celles de la suite  $y_1$  sont les mêmes. L'évaluation de la suite  $y_0$ , qui réclame à priori une division à chaque étape se ramène donc à une suite d'additions-soustractions et de comparaisons à la valeur  $12=17-5$  selon le principe suivant.

*"Partir de la valeur nulle et ajouter 5 à la somme en cours si celle-ci est inférieure à 12, retrancher 12 sinon".*

C'est exactement le principe de l'addition avec retenue. L'algorithme de parcours s'en déduit en fonction des primitives de déplacement horizontal  $\delta h$  et diagonal  $\delta d$  qui consistent respectivement à passer du point  $(x,y) \in \mathbb{Z}^2$  au point  $(x+1,y)$  et au point  $(x+1,y+1)$ .

```

    Algorithmme de parcours des droites naïves
    x=0; y=0; r=0;
    for i=0 to b-1 do
        if r<b-a then begin r=r+a;   x=x+1           end
                       else begin r=r-b+a; x=x+1; y=y+1 end;
    
```

Le tracé d'une droite naïve quelconque s'obtient en initialisant r avec une valeur quelconque de l'intervalle [0,b-1] et en prenant un point initial  $(x_0, y_0)$  quelconque dans  $\mathbb{Z}^2$ .

2 Le parcours des droites \*-connexes.

La définition de ces droites montre qu'elles sont constituées de  $\omega$  pointillés,  $b < \omega < a+b$ , c'est-à-dire d'une droite naïve sur laquelle d'autres points ont été accolés à l'endroit des sauts diagonaux changeant, en ceux-ci, la 8-connexité en 4-connexité. Une droite \*-connexe n'est donc plus "fonctionnelle": elle n'admet plus de paramétrage  $(x, f(x))$  où f est une application puisque au dessus d'un point d'abscisse x il peut exister un ou deux points. Là encore les premières propriétés des droites \*-connexes seront obtenues par leurs suites de restes associées  $r(x,y) = \left\{ \frac{ax+by}{\omega} \right\}$  qui désignent  $ax+by$  modulo  $\omega$ . Il est alors clair que la droite discrète \*-connexe d'équation  $\left[ \frac{ax+by}{\omega} \right] = 0$  s'obtient par le parcours suivant, qui généralise celui des droites naïves.

Considérons la suite  $R_i$  définie par

$$R_0 = 0, \text{ et plus généralement}$$

$$R_{i+1} = \begin{cases} R_i + a & \text{si } 0 \leq R_i < \omega - a \\ R_i - b + a & \text{si } \omega - a \leq R_i < b \\ R_i - b & \text{si } b \leq R_i < \omega. \end{cases}$$

alors celle-ci donne toutes les valeurs des restes qui apparaissent dans une période de la droite \*-connexe considérée et de plus les trois cas envisagés correspondent exactement aux trois déplacements  $\delta h$ ,  $\delta d$  et  $\delta v$  (vertical) qui font passer d'un point de la droite au suivant. Ce choix parmi trois éventualités contraste avec les deux du parcours d'une droite naïve.

Nous en déduisons l'algorithme de tracé suivant de la droite \*-connexe d'équation  $\left[ \frac{ax+by}{\omega} \right] = 0$  et laissons les autres cas au lecteur. Nous remarquons que si  $0 < a < b$  l'équation de cette droite correspond à une droite de pente  $-\frac{a}{b}$  ce qui nécessite de changer les signes des déplacements verticaux par rapport à l'algorithme précédent. Les signes doivent se retrouver, dans l'équation ou dans l'algorithme.

```

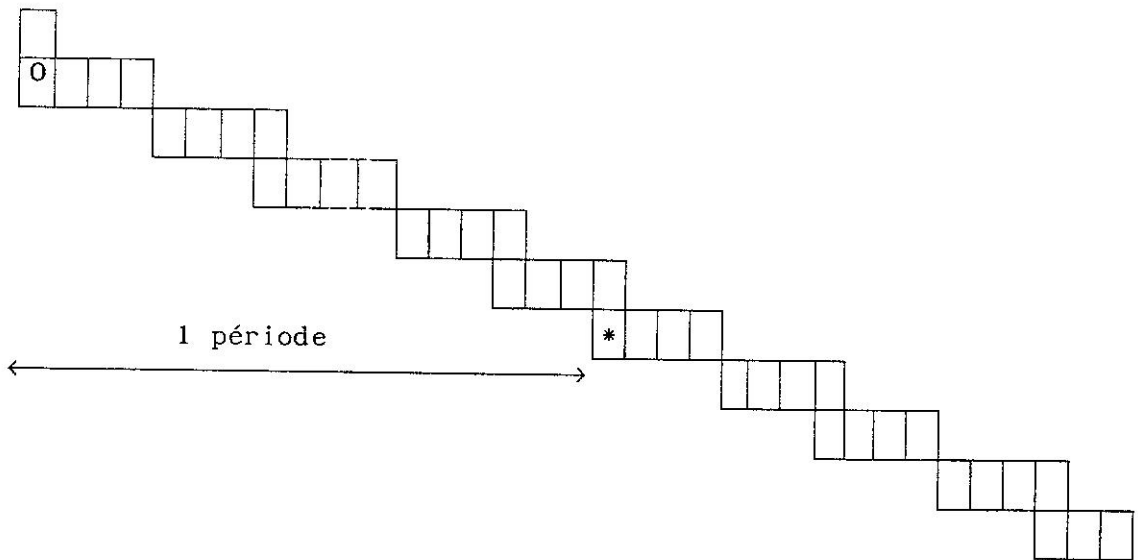
    Algorithme de parcours des droites *-connexes
    x=0; y=0; R=0;
    for i=0 to ω-1 do
        if R<ω-a then begin R=R+a;  x=x+1      end
    else if R<b   then begin R=R-b+a; x=x+1; y=y-1 end
        else begin R=R-b  ; y=y-1      end;

```

Exemple

Donnons le tableau de la suite des restes de la droite d'équation  $\left[\frac{5x+17y}{20}\right]=0$  et le tracé de sa période.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
R <sub>i</sub>	0	5	10	15	3	8	13	18	1	6	11	16	4	9	14	19	2	7	12	17



Le carré repéré par 0 est l'origine de  $\mathbb{Z}^2$   
 Il correspond à une valeur nulle de  $R_1$ .  
 Le point marqué par \* correspond aussi à une  
 valeur  $R_1=0$ .

### 3 Le tracé des droites généralisées: algorithme des vecteurs pilotés.

Nous aurons plusieurs fois recours par la suite à la généralisation évidente du tracé naïf associé au rationnel  $\frac{a}{b}$  obtenu en remplaçant les vecteurs de déplacement  $\delta h=(1,0)$  et  $\delta v=(0,1)$  par deux vecteurs entiers quelconques  $V_1$  et  $V_2$ . Il est clair que la suite de  $\mathbb{Z}^2$  ainsi définie est l'image d'une droite naïve par l'opérateur linéaire de matrice  $(V_1 \ V_2)$ . Nous appellerons algorithme des 2 vecteurs pilotés par le rationnel  $\frac{a}{b}$  la génération d'une telle suite de points. Il est donc obtenu en évaluant la suite des restes  $\{\frac{ai}{b}\}$  et en remplaçant, à partir d'un point initial, chaque valeur inférieure à  $(b-a)$  par un déplacement  $V_1$  et chaque valeur supérieure ou égale à  $(b-a)$  par un déplacement selon  $V_2$ .

Il en est de même pour le tracé  $*$ -connexe associé au rationnel  $\frac{a}{b}$  et à l'épaisseur  $h$  (vérifiant  $b < h < a+b$ ); il se généralise aussi en un tracé de points de  $\mathbb{Z}^2$  obtenu en remplaçant dans la suite des restes  $\{\frac{ai}{b}\}$  les valeurs inférieures à  $b-a$  par  $V_1$ , sinon celles inférieures à  $h-a$  par  $V_1+V_2$  et les autres ( $\geq h-a$ ) par  $V_2$ . Nous appellerons algorithme des 3 vecteurs pilotés par le rationnel  $\frac{a}{b}$  et tronqué par l'épaisseur  $h$  la génération de cette suite de points.

#### Remarque.

Nous pourrions étendre la notion de droite discrète à l'ensemble des points d'un réseau entier contenu dans une bande rationnelle; nous ne le faisons pas, cette généralisation n'intervenant que rarement.

### 4 Le tracé des droites épaisses

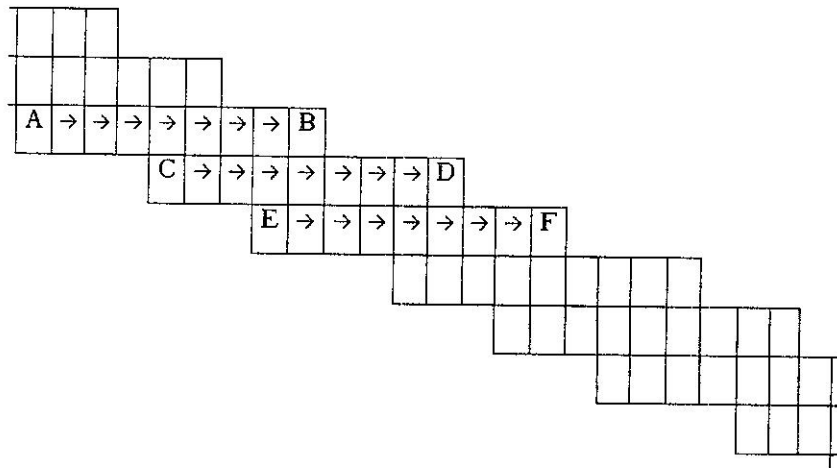
Nous rassemblons ici quelques algorithmes de parcours et de tracé des droites épaisses qui généralisent les précédents. La preuve de la correction de ces algorithmes résultera des premières propriétés des droites discrètes exposées au §IV suivant.

Le tracé des droites épaisses peut être envisagé de deux manières, horizontalement et verticalement, chacune d'elle se dédoublant en un **parcours** de tous les points ou en un **tracé** d'un segment de longueur convenable.

Dans ce paragraphe nous supposons toujours  $0 < a < b$  et  $(a,b)=1$ ; les adaptations nécessaires pour les autres cas sont laissées au lecteur.

L'algorithme de parcours horizontal d'une droite épaisse d'équation  $\left[ \frac{ax+by}{\omega} \right] = 0$ .

Le principe de l'algorithme est illustré par la figure suivante.



Le parcours horizontal d'une droite épaisse décrit les paliers horizontaux dans l'ordre:

A...B, C...D, E...F, etc.

Il nécessite la connaissance des sauts BC, DE,... et de la longueur du palier à parcourir.

L'algorithme proposé est valable sous les hypothèses suivantes:

$0 \leq |a| \leq b$ , même si a et b ne sont pas premiers entre eux,

l'épaisseur  $\omega \geq \sup(|a|, |b|)$ ; (une généralisation à  $\omega$  quelconque est possible, elle passe par l'étude des "bases euclidiennes" présentées plus loin).

Nous introduisons les quantités suivantes:

$$\alpha_1 = \omega - a, \quad \alpha_2 = \alpha_1 + \left\{ \frac{b - \left\lfloor \frac{\omega}{a} \right\rfloor}{a} \right\}, \quad L = \left\lfloor \frac{\omega - b - 1}{a} \right\rfloor \quad \text{et} \quad \ell = \left\lfloor \frac{\omega - b}{a} \right\rfloor - 1,$$

l'algorithme, analogue au cas \*-connexe, s'en déduit.

Algorithme de parcours horizontal

```

x=0; y=0; R=0;
for i=0 to w-1 do
    if R <  $\alpha_1$  then begin R=R+a;    x=x+1    end
    else if R <  $\alpha_2$  then begin R=R- $\alpha_2$ +a; x=x- $\ell$ ; y=y-1 end
    else begin R=R- $\alpha_2$ ;    x=x-L; y=y-1 end;

```

Remarques:

o Cet algorithme donne le parcours d'une période ( $\omega$  points) de la droite épaisse; la droite étant constituée de translatés, par le vecteur  $(b, -a)$ ,

d'une de ses périodes, le parcours se prolonge sans difficulté.

o Les conditions initiales de  $x, y, R$  sont celles du tracé de  $\mathcal{D}(a, b, 0, \omega)$ ; elles peuvent être calculées pour le tracé de toute droite  $\mathcal{D}(a, b, \gamma, \omega)$ ,  $\gamma$  étant quelconque. La nouvelle droite est la translatée, par le vecteur  $(\tau_x, \tau_y)$  de la droite épaisse où  $\gamma=0$ ,  $\tau_x$  et  $\tau_y$  étant donnés par les relations

$$\tau_x = \left\{ \frac{\gamma u}{b} \right\} \quad \text{et} \quad \tau_y = a \left[ \frac{\gamma u}{b} \right] + \gamma v$$

u et v étant les coefficients de Bezout de a et b, i.e.  $au+bv=1$ .

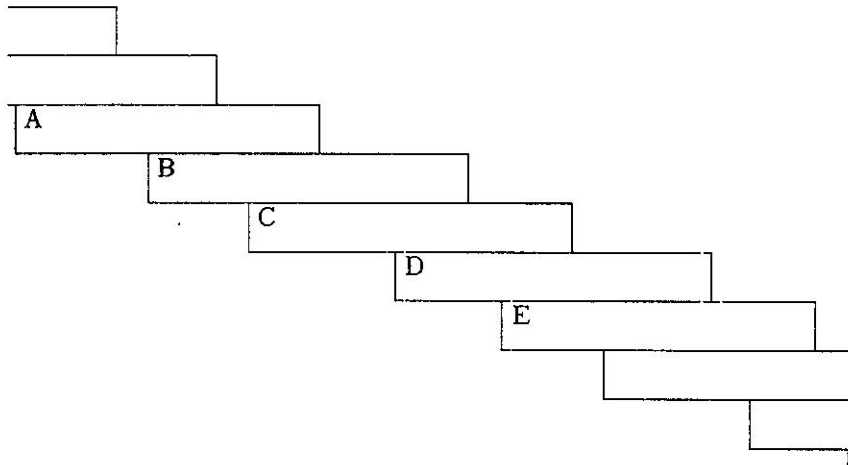
o On peut utiliser les symétries des droites discrètes pour s'affranchir de la restriction  $0 \leq |a| \leq b$  et tracer une droite épaisse quelconque.

Le tracé horizontal d'une droite épaisse d'équation  $\left[ \frac{ax+by}{\omega} \right] = 0$ .

L'algorithme consiste à tracer des segments horizontaux de longueur  $\ell = \left[ \frac{\omega}{a} \right]$  ou  $L = \ell + 1$  (cas  $\left\{ \frac{\omega}{a} \right\} \neq 0$ ) à partir de la suite de points A, B, ... débuts de paliers

de la droite naïve de même pente. Ici cette suite n'est pas générée par  $\left\{ \frac{ai}{b} \right\}$

mais par la suite arithmétique  $\left\{ \frac{(a - \left\{ \frac{b}{a} \right\})i}{a} \right\}$ .



Le tracé horizontal d'une droite épaisse remplit les paliers horizontaux dans l'ordre:

A, B, C, D, E...

Il nécessite la connaissance des sauts AB, BC, CD, ... et de la longueur du segment à tracer.

Cet algorithme comprend deux cas,  $\left\{ \frac{\omega}{a} \right\} < \left\{ \frac{b}{a} \right\}$  et  $\left\{ \frac{\omega}{a} \right\} > \left\{ \frac{b}{a} \right\}$ .

Nous posons  $\ell = \left[ \frac{\omega}{a} \right]$  et  $L = \ell + 1$  si  $\left\{ \frac{\omega}{a} \right\} \neq 0$  et  $L = \ell$  sinon; de même  $\lambda = \left[ \frac{b}{a} \right]$  et  $\Lambda = \lambda + 1$  si  $\left\{ \frac{b}{a} \right\} \neq 0$  et  $\Lambda = \lambda$  sinon.

Nous convenons de désigner par la locution "tracer L" (resp. tracer  $\ell$ ) la

primitive qui permet de tracer un segment horizontal de longueur L (resp.  $\ell$ ).

Si  $\{\frac{\omega}{a}\} < \{\frac{b}{a}\}$  l'algorithme est le suivant

```

    Algorithme de tracé horizontal (cas  $\{\frac{\omega}{a}\} < \{\frac{b}{a}\}$ )
x=0; y=0; R=0;
for i=0 to a-1 do
    if  $R < \{\frac{\omega}{a}\}$  then begin  $R=R+a-\{\frac{b}{a}\}$ ; tracer L;  $x=x+\Lambda$ ;  $y=y-1$  end
else if  $R < \{\frac{b}{a}\}$  then begin  $R=R+a-\{\frac{b}{a}\}$ ; tracer  $\ell$ ;  $x=x+\Lambda$ ;  $y=y-1$  end
    else begin  $R=R-\{\frac{b}{a}\}$ ; tracer  $\ell$ ;  $x=x+\lambda$ ;  $y=y-1$  end;

```

Si  $\{\frac{\omega}{a}\} > \{\frac{b}{a}\}$  l'algorithme s'écrit

```

    Algorithme de tracé horizontal (cas  $\{\frac{\omega}{a}\} > \{\frac{b}{a}\}$ )
x=0; y=0; R=0;
for i=0 to a-1 do
    if  $R < \{\frac{b}{a}\}$  then begin  $R=R+a-\{\frac{b}{a}\}$ ; tracer L;  $x=x+\Lambda$ ;  $y=y-1$  end
else if  $R < \{\frac{\omega}{a}\}$  then begin  $R=R-\{\frac{b}{a}\}$ ; tracer L;  $x=x+\lambda$ ;  $y=y-1$  end
    else begin  $R=R-\{\frac{b}{a}\}$ ; tracer  $\ell$ ;  $x=x+\lambda$ ;  $y=y-1$  end;

```

Cet algorithme est particulièrement intéressant pour les applications graphiques puisqu'il donne la période de la droite discrète en a opérations indépendamment de l'épaisseur  $\omega$  de la droite.

L'algorithme de parcours vertical d'une droite épaisse d'équation  $\left[ \frac{ax+by}{\omega} \right] = 0$ .

En introduisant les constantes suivantes

$$\beta_1 = \omega - b, \quad \beta_2 = \beta_1 + \left\{ \frac{-a - \{\frac{\omega}{b}\}}{b} \right\}, \quad L = \left[ \frac{\omega + a - 1}{b} \right] \quad \text{et} \quad \ell = \left[ \frac{\omega + a}{b} \right]$$

nous obtenons l'algorithme de parcours vertical d'une période de la droite discrète  $\mathcal{D}(a,b,0,\omega)$ , analogue au parcours horizontal; il prend la forme:

```

    Algorithme de parcours vertical
x=0; y=0; R=0;
for i=0 to w-1 do
    if  $R < \beta_1$  then begin  $R=R+b$ ;  $y=y+1$  end
else if  $R < \beta_2$  then begin  $R=R-\beta_2+b$ ;  $x=x+1$ ;  $y=y-\ell$  end
    else begin  $R=R-\beta_2$ ;  $x=x+1$ ;  $y=y-L$  end;

```

Sous cette forme simplifiée il est valable pour  $0 \leq |a| \leq b$ . Les mêmes remarques que celles qui suivent l'algorithme de parcours horizontal sont valables.

Le tracé vertical d'une droite épaisse d'équation  $\left[ \frac{ax+by}{\omega} \right] = 0$ .

Conjointement aux valeurs  $\ell$  et  $L$  précédentes nous introduisons  $\lambda=0$  et  $\Lambda=1$  (l'hypothèse  $0 < a < b$  est responsable de quelques dissymétries par rapport au tracé horizontal); le tracé vertical fait apparaître deux cas.

Pour  $\left\{ \frac{\omega}{b} \right\} < \left\{ \frac{-a}{b} \right\}$  l'algorithme s'écrit:

Algorithme de tracé vertical (cas  $\left\{ \frac{\omega}{b} \right\} < \left\{ \frac{-a}{b} \right\}$ )

```

x=0; y=0; R=0;
for i=0 to b-1 do
    if R < { ω / b } then begin R=R+a;      tracer L; x=x+1; y=y-λ end
else if R < { -a / b } then begin R=R+a-b;  tracer L; x=x+1; y=y-Λ end
                                else begin R=R+a-b;      tracer ℓ; x=x+1; y=y-Λ end;

```

alors que pour  $\left\{ \frac{\omega}{b} \right\} > \left\{ \frac{-a}{b} \right\}$  il est donné par

Algorithme de tracé vertical (cas  $\left\{ \frac{\omega}{b} \right\} > \left\{ \frac{-a}{b} \right\}$ )

```

x=0; y=0; R=0;
for i=0 to b-1 do
    if R < { -a / b } then begin R=R+a;      tracer L; x=x+1; y=y-λ end
else if R < { ω / b } then begin R=R+a;      tracer ℓ; x=x+1; y=y-λ end
                                else begin R=R+a-b;      tracer ℓ; x=x+1; y=y-Λ end;

```

#### IV LES PROPRIÉTÉS MODULAIRES DES DROITES DISCRÈTES.

Nous réunissons ici les notions et propriétés des droites discrètes liées à l'étude de la suite arithmétique des restes  $\left\{ \frac{ai}{b} \right\}$ ; ce sont les propriétés modulaires des droites discrètes.

Loger la géométrie dans  $\mathbb{Z}^2$  impose d'apprendre à lire dans l'une ou l'autre des suites  $\left[ \frac{ai}{b} \right]$  ou  $\left\{ \frac{ai}{b} \right\}$ , transcodages mutuels, le plus grand nombre de propriétés des droites discrètes. Il s'avère que la deuxième, algébriquement structurée, est plus commode. Il suffit en fait de se laisser piloter par son contenu arithmétique qui contrôle entièrement la géométrie de ces droites. Ce traitement prolonge d'ailleurs celui de Christoffel [22]. Nous devons à la fois réinterpréter géométriquement certains résultats arithmétiques et traduire arithmétiquement certaines propriétés géométriques; bref il faut écrire quelque peu cette équivalence.

Comme nous visons d'utiliser nos résultats pour accélérer certains traitements sur machine nous devons éviter de recourir aux outils trop sophistiqués et travailler à un niveau très élémentaire; ce qui se paie souvent en longueurs.

Reprenant une idée de Jean Bernoulli, Christoffel a le premier associé un mot sur deux lettres à tout rationnel et relié la structure de ce mot au développement en fraction continue de ce rationnel. Or ce mot s'interprète géométriquement en terme de droite naïve ce qui confirme le rôle naturel de cette notion dans l'étude des propriétés des droites discrètes et de leurs relations avec les fractions continues. Les propriétés des mots de Christoffel ont été démontrées indépendamment par l'un de ses contemporains [110]. Signalons aussi les travaux récents d'Earnshaw-Pitteway [39] et de J.Berstel [5] sur cette approche mais pour le mot de Christoffel associé à la droite discrète de meilleure approximation entière.

L'implémentation sur ordinateur de ces algorithmes sera avantagée si la description de la structure d'une droite discrète est faite par le mot le plus court possible. Pour une droite naïve de pente  $\frac{a}{b}$ ,  $a$  et  $b$  vérifiant les inégalités  $0 < a < b$  nous constatons que le mot de paliers de longueur  $a$  de ces droites formé par les lettres  $l$  et  $c$  hérite naturellement de celles du mot de Christoffel. Sa structure se lit directement sur le développement en fraction continue de  $\frac{a}{b}$ . Cette approche présente l'avantage supplémentaire de supprimer quelques étapes de l'algorithme d'Euclide et raccourcit donc la construction du mot de paliers. Ce mot a également été étudié par Dulucq et Gouyou-Beauchamp [38]. Nous retrouvons des résultats connus de ces chercheurs ainsi que de Hung [61] et Wu [120] mais par des voies différentes.

## 1 Le mot de CHRISTOFFEL et le mot de paliers d'un rationnel

La suite des restes  $\left\{ \frac{ai}{b} \right\}$ , possède dans l'intervalle  $[0, b-1]$ , constituant une période,  $a$  séquences montantes maximales correspondant aux paliers de la droite naïve de pente  $\frac{a}{b}$ .

A tout rationnel  $\frac{a}{b}$  Christoffel associe la suite des montées et descentes, symbolisées par les lettres  $c$  et  $d$ , de la suite des restes  $r_i = \left\{ \frac{ai}{b} \right\}$  où  $i=1, \dots, b$ . Plus précidément il définit le mot  $l_1 l_2 l_3 \dots l_b$  où  $l_i$  est la lettre  $c$  si  $r_i < r_{i+1}$  et la lettre  $d$  si  $r_i > r_{i+1}$ , utilisant la périodicité de la suite  $r_i$  pour définir  $l_b$ . Observant que les deux dernières lettres sont toujours  $dc$  il appelle partie principale, ce que nous notons  $Ch\left(\frac{a}{b}\right)$  et appelons le mot de Christoffel de  $\frac{a}{b}$ , le sous-mot  $l_1 l_2 l_3 \dots l_{b-2}$ . Ce mot décrit donc les séquences montantes de la suite  $r_i$  qui correspondent aux paliers de la droite naïve de

penne  $\frac{a}{b}$ . Christoffel et Smith donnent la relation existant entre le rationnel  $\frac{a}{b}$  et le mot qui lui est associé, permettant de passer de l'un à l'autre. La relation s'exprime à l'aide du développement en fraction continue de  $\frac{a}{b}$ .

Le théorème de Christoffel-Smith est le suivant.

Si  $\alpha=[s, s_1, s_2, \dots, s_n]$  est le développement en fraction continue de  $\alpha=\frac{a}{b}$ , où  $\alpha \in [0, 1]$ , alors le mot de Christoffel de  $\alpha$ ,  $Ch(\alpha)$ , est obtenu par la construction suivante. Déterminer les suites de mots  $\gamma_n$ ,  $c_n$  et  $d_n$  selon les récurrences

$$\begin{aligned} \gamma &= c^{s-1} & c_1 &= c^{s-1}d & d_1 &= c^s d \\ \gamma_1 &= c_1^{s_1-1} & c_2 &= c_1^{s_1-1}d_1 & d_2 &= c_1^{s_1}d_1 \\ \gamma_2 &= c_2^{s_2-1} & c_3 &= c_2^{s_2-1}d_2 & d_3 &= c_2^{s_2}d_2 \\ & & & \dots & & \end{aligned}$$

Ensuite nous avons  $Ch(\alpha) = c_1 c_2 \dots c_{n-1} \gamma_n \gamma_{n-1} \dots \gamma_2 \gamma_1 \gamma$ .

Par exemple

$$\frac{7}{24} = \frac{1}{3 + \frac{1}{2 + \frac{1}{3}}}$$

d'où  $s=3$ ,  $s_1=2$ ,  $s_2=3$ ,  $n=2$ , le mot de Christoffel est

$$Ch(\alpha) = c_1 \gamma_2 \gamma_1 \gamma$$

et  $\gamma = c^2$ ,  $c_1 = c^2 d$ ,  $d_1 = c^3 d$ ,  $\gamma_1 = c_1$ ,  $c_2 = c_1 d_1$ ,  $\gamma_2 = c_2^2 = c_1 d_1 c_1 d_1$ , d'après les relations (1), d'où

$$Ch(\alpha) = c_1 c_1 d_1 c_1 d_1 c_1 \gamma$$

en remplaçant en fonction de  $c$  et  $d$  nous obtenons

$$Ch(\alpha) = c^2 d c^2 d c^3 d c^2 d c^3 d c^2 d c^2$$

Comparons plus précisément cette expression à la suite des paliers longs et courts de la droite naïve de pente  $\frac{7}{24}$ . La suite  $r_i$ ,  $i=0, \dots, b-1$ , étant

0, 7, 14, 21, 4, 11, 18, 1, 8, 15, 22, 5, 12, 19, 2, 9, 16, 23, 6, 13, 20, 3, 10, 17

en associant les lettres  $l$  et  $c$  aux paliers longs et courts nous pouvons former le mot  $lclclcc$ ; nous le retrouvons à partir du mot  $c\overset{7}{\text{Ch}}(\text{---})d$  obtenu en encadrant le mot de Christoffel des lettres  $c$  et  $d$  et en remplaçant les mots  $c^3d$  par  $l$  et  $c^2d$  par  $c$ . Le mot  $lclclcc$  est formé de  $a$  lettres au lieu de  $b-2$ , c'est une condensation du mot de Christoffel. Ceci nous conduit à la notion suivante

### Définition 1

Nous appelons mot de paliers de  $\frac{a}{b}$ , noté  $\mu(\frac{a}{b})$ , le mot sur les lettres  $l$  et  $c$  obtenu en remplaçant respectivement les paliers longs et courts de la période de la droite naïve de pente  $\frac{a}{b}$  par  $l$  et  $c$ ; ce mot est de longueur  $a$ .

L'exemple précédent a pour mot de paliers:

$$\mu(\frac{7}{24}) = lclclcc$$

### 2 L'algorithme de Christoffel.

Nous pouvons déduire immédiatement du théorème de Christoffel un algorithme de tracé d'une droite discrète naïve surtout commode pour les tracés à la main.

Désignons ici par  $\mathcal{D}$  la droite naïve de pente  $\frac{a}{b}$  où  $0 \leq a < b$ ,  $a$  et  $b$  premiers entre eux; on peut toujours, par des symétries, se ramener à ce cas. Désignons par  $[q_1, q_2, \dots, q_n] = \frac{a}{b}$  le développement en fraction continue de la pente  $\frac{a}{b}$  et par  $P_i$  la période du tracé de la droite naïve de pente  $[q_1, q_2, \dots, q_i]$  pour  $1 \leq i \leq n$ . Le théorème de Christoffel s'interprète géométriquement par la relation

$$P_{i+1} = q_{i+1} P_i + P_{i-1} \quad \text{où } i=0, \dots, n-1$$

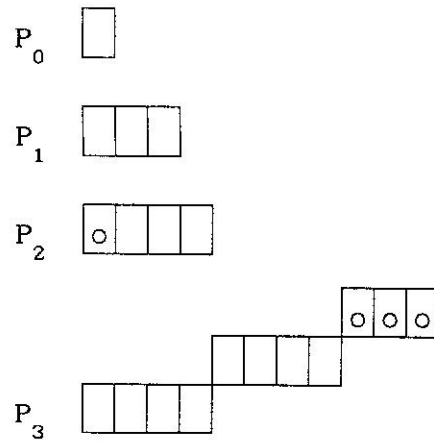
avec les conventions suivantes:

$P_{-1} = \emptyset$ ,  $P_0$  est réduit à un point,  $P_1$  est un segment horizontal de  $q_1$  points consécutifs, la somme étant interprétée vectoriellement et effectuée de gauche à droite si  $i$  est pair et de droite à gauche sinon.

Donnons quelques exemples qui éclairciront le mécanisme de cet algorithme.

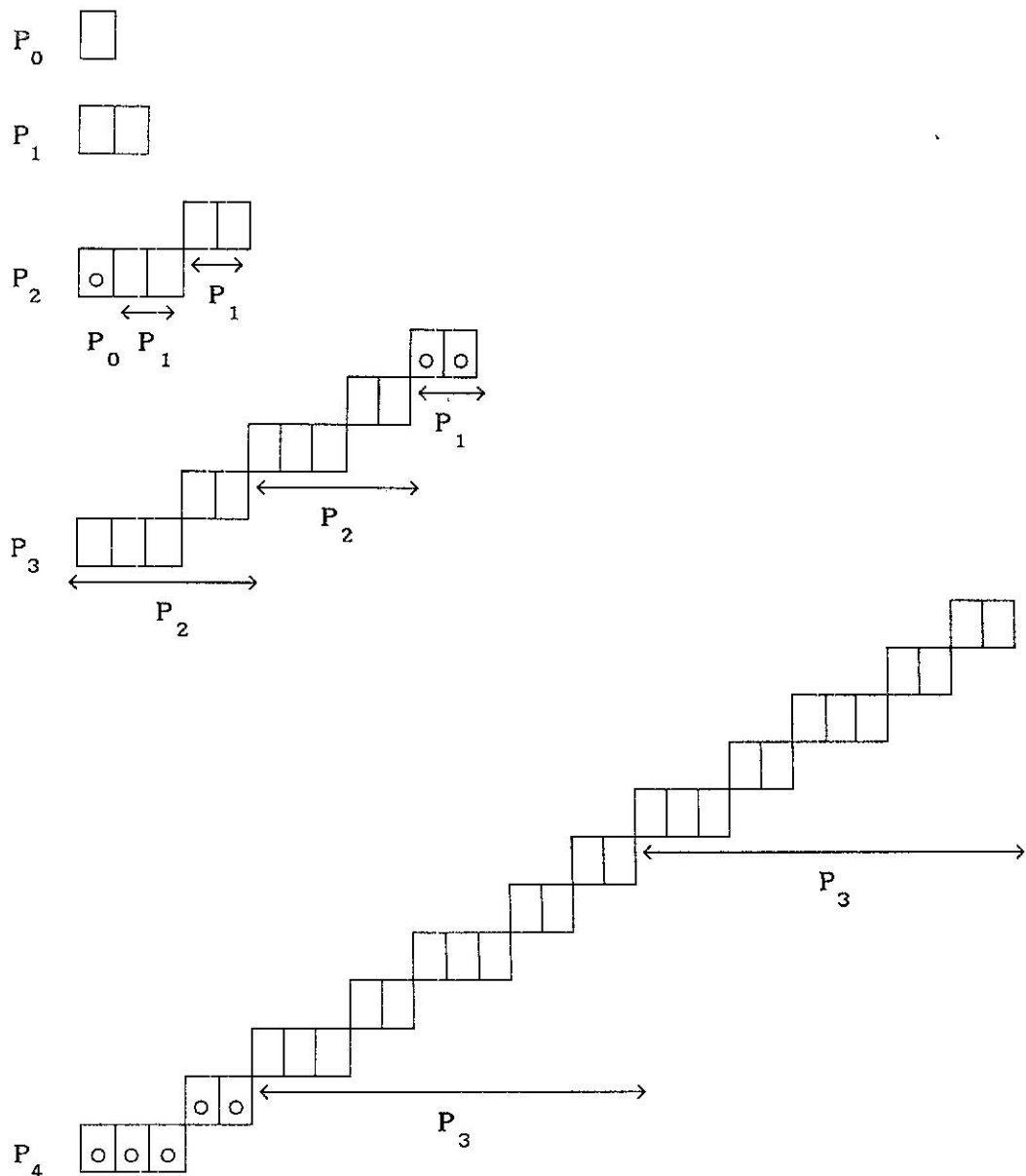
### Exemples.

a) Construisons la période de la droite naïve de pente  $\frac{3}{11} = [3, 1, 2]$ . Les diverses étapes  $P_i$   $i=0, 1, 2, 3$  sont représentées ci-dessous.



Les points marqués sont ceux de  $P_{i-1}$ . La structure de  $P_3 = 2 P_2 + P_1$  par exemple se lit, comme  $i=2$  est pair, de gauche à droite; elle est constituée de  $q_3=2$  exemplaires de  $P_2$  et d'un exemplaire de  $P_1$  juxtaposés par leurs sommets.

b) Appliquons cet algorithme pour construire la période de  $\frac{19}{29}=[2,2,2,2]$ . Représentons les  $P_i$  selon les mêmes principes.



### 3 Les séquences montantes d'une droite naïve

Reprenons notre étude de la suite des restes. Nous constatons immédiatement que les séquences montantes de la suite  $\left\{\frac{ai}{b}\right\}$  commencent par une valeur appartenant à l'intervalle  $[0, a-1]$  et se terminent par une valeur dans  $[b-a, b-1]$ . Nous allons préciser les longueurs des séquences montantes de la suite  $\left\{\frac{ai}{b}\right\}$  dans l'intervalle  $[0, b-1]$ . Donnons un exemple avant d'énoncer les résultats.

#### Exemple

Reprenons le rationnel  $\frac{7}{24}$ , utilisé plus haut, en désignant respectivement par  $Y_0$  et  $Y_1$  les suites  $\left[\frac{ai}{b}\right]$  et  $\left\{\frac{ai}{b}\right\}$ .

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
$Y_0$	0	0	0	0	1	1	1	2	2	2	2	3	3	3	4	4	4	4	5	5	5	6	6	6
$Y_1$	0	7	14	21	4	11	18	1	8	15	22	5	12	19	2	9	16	23	6	13	20	3	10	17

Les séquences montantes de la suite  $Y_1$  sont 0,7,14,21 puis 4,11,18, puis 1,8,15,22, etc... Les débuts des séquences montantes sont 0,4,1,5,2,6 et 3; les fins de ces séquences sont 21,18,22,19,23,20 et 17.

Regardons les longueurs des séquences montantes.

proposition 1

- a) Les longueurs des séquences montantes de la suite  $\left\{\frac{ai}{b}\right\}$  sont égales à  $\left[\frac{b}{a}\right]$  ou à  $\left[\frac{b}{a}\right]+1$ .
- b) L'entier  $i$  est un début (resp. une fin) de palier ssi  $0 < \left\{\frac{ai}{b}\right\} < a$  (resp.  $b-a < \left\{\frac{ai}{b}\right\} < b$ ).

Démonstration:

Comme chaque séquence montante débute par une valeur  $k \in [0, a-1]$  sa longueur est donnée par l'expression

$$1 + \left[\frac{b-k}{a}\right]$$

Evaluons les entiers  $\left[\frac{b-k}{a}\right]$  lorsque  $k$  parcourt  $[0, a-1]$ ; par définition de  $\left[\frac{b}{a}\right]$  et  $\left\{\frac{b}{a}\right\}$  l'égalité de division euclidienne de  $b$  par  $a$  s'écrit

$$b = \left[\frac{b}{a}\right]a + \left\{\frac{b}{a}\right\}$$

ou encore

$$\frac{b - \left\{\frac{b}{a}\right\}}{a} = \left[\frac{b}{a}\right]$$

Par conséquent  $\frac{b-k}{a}$  est entier si et seulement si  $k$  est de la forme  $\left\{\frac{b}{a}\right\} + ma$  où  $m$  est dans  $\mathbb{Z}$ . En particulier si  $k \in \left[\left\{\frac{b}{a}\right\}+1, \left\{\frac{b}{a}\right\}+a\right]$  ou si  $k \in \left[\left\{\frac{b}{a}\right\}-a+1, \left\{\frac{b}{a}\right\}\right]$

la partie entière  $\left[ \frac{b-k}{a} \right]$  est constante. Le dernier intervalle introduit contient l'intervalle  $[1, \left\{ \frac{b}{a} \right\}]$  puisque  $\left\{ \frac{b}{a} \right\} < a$ . Nous en déduisons immédiatement les égalités suivantes:

$$\left[ \frac{b-1}{a} \right] = \left[ \frac{b-2}{a} \right] = \dots = \left[ \frac{b - \left\{ \frac{b}{a} \right\}}{a} \right] = \left[ \frac{b}{a} \right] \quad (1)$$

et

$$\left[ \frac{b - \left\{ \frac{b}{a} \right\} - 1}{a} \right] = \dots = \left[ \frac{b-a}{a} \right] = \left[ \frac{b}{a} \right] - 1. \quad (2)$$

Ceci montre que les longueurs des séquences montantes de la suite  $\left\{ \frac{a_i}{b} \right\}$  sont égales à  $\left[ \frac{b}{a} \right] + 1$  ou à  $\left[ \frac{b}{a} \right]$  et prouve a); b) s'en déduit.

Bien que les longueurs des séquences montantes soient deux entiers consécutifs nous dirons que celles de longueur  $\left[ \frac{b}{a} \right]$  sont courtes et les autres longues. Comme le premier terme de la première séquence montante est 0 le premier palier est long; comme le début de la dernière séquence montante est  $\left\{ \frac{b}{a} \right\}$  (retrancher a autant qu'il est possible à b tout en restant positif), celle-ci est toujours courte.

### proposition 2

*La première séquence montante est longue, la dernière est courte.*

Les relations (1) et (2) précédentes permettent d'étudier assez précisément la répartition des paliers des deux types. Nous avons le résultat suivant

### proposition 3

*Les propriétés suivantes sont équivalentes:*

- i) Une séquence montante  $\alpha, \alpha+a, \dots, \beta$  est longue.
- ii)  $\alpha \in [0, \left\{ \frac{b}{a} \right\} - 1]$ .
- iii)  $\beta \in [b - \left\{ \frac{b}{a} \right\}, b-1]$ .

*De même les propriétés suivantes sont équivalentes:*

- i) Une séquence montante  $\alpha, \alpha+a, \dots, \beta$  est courte.

$$\text{ii) } \alpha \in \left[ \left\{ \frac{b}{a} \right\}, a-1 \right].$$

$$\text{iii) } \beta \in [b-a, b - \left\{ \frac{b}{a} \right\} - 1].$$

En particulier le nombre de longues séquences montantes est  $\left\{ \frac{b}{a} \right\}$ , celui des courtes est  $a - \left\{ \frac{b}{a} \right\}$ .

Remarque.

Dans le cas particulier où  $\left\{ \frac{b}{a} \right\} = b-a$ , les intervalles  $\left[ \left\{ \frac{b}{a} \right\}, a-1 \right]$  et  $[b-a, b - \left\{ \frac{b}{a} \right\} - 1]$  coïncident.

Nous déduisons de la proposition 2 la

proposition 4

Le début de la deuxième séquence montante vaut  $a - \left\{ \frac{b}{a} \right\}$ .

proposition 5

La suite des débuts des séquences montantes est la suite  $\left\{ \frac{(a - \left\{ \frac{b}{a} \right\})i}{a} \right\}$ .

Démonstration:

Montrons que si  $\alpha$  est le début d'une séquence montante longue le début de la séquence montante suivante est  $\alpha + a - \left\{ \frac{b}{a} \right\}$ ; si  $\alpha$  est le début d'une séquence montante courte le début de la séquence montante suivante est  $\alpha - \left\{ \frac{b}{a} \right\}$ .

En effet si  $\alpha$  est le début d'une séquence montante courte,  $\alpha \geq \left\{ \frac{b}{a} \right\}$  comme nous venons de le voir, de plus le début de la séquence montante suivante vaut  $\left[ \frac{b}{a} \right] a + \alpha - b$  qui coïncide avec  $\alpha - \left\{ \frac{b}{a} \right\}$ ; ce calcul a bien un sens. Si  $\alpha$  est le début d'une séquence montante longue le début de la séquence montante suivante est  $\left[ \frac{b}{a} \right] a + a + \alpha - b = \alpha + a - \left\{ \frac{b}{a} \right\}$  qui est bien majoré par  $a-1$  puisque  $\alpha \leq \left\{ \frac{b}{a} \right\} - 1$  ■

#### 4 Un algorithme de tracé par paliers

Soit  $l...c = \mu\left(\frac{a}{b}\right)$  le mot de paliers du rationnel  $\frac{a}{b}$ , l'ordre des paliers et leur type  $l$  ou  $c$  est donc donné par la suite arithmétique  $\rho_i = \left\{ \frac{(a - \left\langle \frac{b}{a} \right\rangle)i}{a} \right\}$  et par la comparaison de ses valeurs au seuil  $\left\langle \frac{b}{a} \right\rangle$ : si  $0 \leq \rho_i < \left\langle \frac{b}{a} \right\rangle$  le palier est long, si  $\left\langle \frac{b}{a} \right\rangle \leq \rho_i < a$  le palier est court. Nous pouvons déduire de ces remarques un algorithme de tracé par paliers de la période d'une droite naïve en supposant que les primitives `trace_palier_court` et `trace_palier_long` tracent un segment horizontal de longueurs respectives  $\left[ \frac{b}{a} \right]$  et  $\left[ \frac{b}{a} \right] + 1$  à partir de la position  $(x,y)$  initialement à  $(0,0)$ .

```

    Algorithme de tracé par paliers longs et courts
x=0; y=0; R=0;
For i=1 to a do
    begin
        if R <  $\left\langle \frac{b}{a} \right\rangle$  then
            begin
                tracer palier_long;
                x=x +  $\left[ \frac{b}{a} \right] + 1$ ; R=R+a -  $\left\langle \frac{b}{a} \right\rangle$ 
            end
        else
            begin
                tracer palier_court;
                x=x +  $\left[ \frac{b}{a} \right]$ ; R=R -  $\left\langle \frac{b}{a} \right\rangle$ 
            end;
        y=y+1
    end;

```

#### 5 La structure du mot de paliers

Appliquons la proposition 5 à la recherche du début de la deuxième séquence montante longue. Si  $a - \left\langle \frac{b}{a} \right\rangle < \left\langle \frac{b}{a} \right\rangle$  la deuxième séquence montante est longue, sinon  $a - \left\langle \frac{b}{a} \right\rangle + a - \left\langle \frac{b}{a} \right\rangle \geq a$  donc le terme suivant de la suite  $\left\{ \frac{(a - \left\langle \frac{b}{a} \right\rangle)i}{a} \right\}$  vaut  $a - 2 \left\langle \frac{b}{a} \right\rangle$ , puis  $a - 3 \left\langle \frac{b}{a} \right\rangle, \dots$  Ce calcul est répété tant que  $a - k \left\langle \frac{b}{a} \right\rangle \geq \left\langle \frac{b}{a} \right\rangle$  ie tant que la suite dépasse la valeur  $\left\{ \frac{a - \left\langle \frac{b}{a} \right\rangle}{\left\langle \frac{b}{a} \right\rangle} \right\} = \left\{ \frac{a}{\left\langle \frac{b}{a} \right\rangle} \right\}$ . Il en résulte:

proposition 6

La suite des débuts des longues séquences montantes est donnée par l'expression

$$\left\{ \frac{\left\{ \frac{a}{\left\{ \frac{b}{a} \right\} i} \right\}}{\left\{ \frac{b}{a} \right\}} \right\} \quad 0 \leq i \leq \left\{ \frac{b}{a} \right\} - 1$$

De même la suite des débuts des séquences montantes courtes est donnée par la suite:

$$\left\{ \frac{\left\{ \frac{b}{a} \right\} i}{a - \left\{ \frac{b}{a} \right\}} \right\} \quad 1 \leq i \leq a - \left\{ \frac{b}{a} \right\} - 1$$

suivie du terme  $a - \left\{ \frac{b}{a} \right\}$ , parcourue à l'envers.

Exemple.

Regardons la suite  $\left\{ \frac{11 \cdot i}{24} \right\}$ , dont les 24 premières valeurs sont:

0 11 22 9 20 7 18 5 16 3 14 1 12 23 10 21 8 19 6 17 4 15 2 13

Les séquences montantes longues sont 0 11 22 et 1 12 23,

les courtes sont 9 20, 7 18, 5 16, 3 14, 10 21, 8 19, 6 17, 4 15, 2 13,

au nombre respectif de  $2 = \left\{ \frac{24}{11} \right\}$  et  $9 = 11 - \left\{ \frac{24}{11} \right\}$ .

Les débuts de séquences montantes, qui valent 0,9,7,5,3,1,10,8,6,4,2 sont bien

donnés par la suite  $\left\{ \frac{9i}{11} \right\}$  alors que la suite des débuts des longues séquences

montantes est 0,1, qui coïncide avec la suite  $\left\{ \frac{i}{2} \right\}$  conformément à la

proposition 5 alors que la suite des débuts des séquences montantes courtes lue à l'envers est 2,4,6,8,10,3,5,7 et 9.

Connaissant les nombres de séquences montantes longues ou courtes de la suite

$\left\{ \frac{ai}{b} \right\}$  nous allons dégager une propriété caractéristique de la population la moins nombreuse.

Définition 2

Nous dirons que les séquences montantes longues sont dominantes si  $\left\{\frac{b}{a}\right\} > a - \left\{\frac{b}{a}\right\}$ , ie  $2\left\{\frac{b}{a}\right\} > a$  et que les séquences montantes courtes sont dominantes si  $2\left\{\frac{b}{a}\right\} < a$ .

proposition 7

Dans le mot de paliers associé à la suite  $\left\{\frac{ai}{b}\right\}$ , la lettre non dominante est isolée; ie il ne peut y avoir deux lettres non dominantes consécutives.

Démonstration

Supposons que les courts soient dominants, c'est à dire que l'on ait  $2\left\{\frac{b}{a}\right\} < a$ , il résulte immédiatement de la proposition 3 que le dernier élément d'une séquence montante longue quelconque est élément de l'intervalle  $[b - \left\{\frac{b}{a}\right\}, b-1]$  et que le terme suivant de la suite est compris entre  $a - \left\{\frac{b}{a}\right\}$  et  $a-1$ , donc entre  $\left\{\frac{b}{a}\right\}$  et  $a-1$ , c'est donc le début d'une séquence montante courte. Le raisonnement est analogue dans le cas des longs dominants ■

Nous avons vu que les débuts de séquences montantes sont engendrés par la suite  $\left\{\frac{(a - \left\{\frac{b}{a}\right\})i}{a}\right\}$ . Ce résultat n'est pas indépendant de la proposition précédente car dans le cas où les longs dominent les valeurs de cette suite appartenant à l'intervalle  $[\left\{\frac{b}{a}\right\}, a-1]$  correspondent aux c du mot de paliers, les autres aux lettres l. Ceci montre que le mot de paliers correspond à la suite  $\left\{\frac{(a - \left\{\frac{b}{a}\right\})i}{a}\right\}$  des restes du rationnel  $\frac{a - \left\{\frac{b}{a}\right\}}{a}$ , les séquences montantes de la suite  $\left\{\frac{(a - \left\{\frac{b}{a}\right\})i}{a}\right\}$  étant associées aux sous mots de la forme ll..lc. Dans le cas des courts dominant la suite  $\left\{\frac{(a - \left\{\frac{b}{a}\right\})i}{a}\right\}$  est remplacée par la suite  $\left\{\frac{\left\{\frac{b}{a}\right\}.i}{a}\right\}$  qui correspond au mot de paliers retourné. Finalement il en résulte que les sous-mots formés des lettres dominantes consécutives, les paliers du mot de paliers, ont deux longueurs possibles qui sont des entiers consécutifs. Plus précisément nous avons:

proposition 8

Les longueurs des paliers du mot de paliers sont

$$\left[ \frac{\left\{ \frac{b}{a} \right\}}{a - \left\{ \frac{b}{a} \right\}} \right] \text{ ou } \left[ \frac{\left\{ \frac{b}{a} \right\}}{a - \left\{ \frac{b}{a} \right\}} \right] + 1 \text{ si les séquences montantes longues dominent}$$

et

$$\left[ \frac{a - \left\{ \frac{b}{a} \right\}}{\left\{ \frac{b}{a} \right\}} \right] \text{ ou } \left[ \frac{a - \left\{ \frac{b}{a} \right\}}{\left\{ \frac{b}{a} \right\}} \right] + 1 \text{ si les séquences montantes courtes dominent.}$$

La suite des paliers du mot de paliers  $\mu\left(\frac{a}{b}\right)$  est décrite par la suite des séquences montantes d'un nouveau rationnel.

proposition 9

Les paliers du mot de paliers de  $\frac{a}{b}$  sont décrits par le rationnel  $\frac{a - \left\{ \frac{b}{a} \right\}}{\left\{ \frac{b}{a} \right\}}$

si les longs dominent et par le rationnel  $\frac{\left\{ \frac{b}{a} \right\}}{a - \left\{ \frac{b}{a} \right\}}$  si les courts dominent; dans

ce dernier cas le mot de paliers est parcouru à l'envers. Dans tous les cas le

rationnel associé à  $\frac{a}{b}$  est  $\frac{\inf\left\{ a - \left\{ \frac{b}{a} \right\}, \left\{ \frac{b}{a} \right\} \right\}}{\sup\left\{ a - \left\{ \frac{b}{a} \right\}, \left\{ \frac{b}{a} \right\} \right\}}$ .

Remarque

Nous aurions pu choisir de définir les paliers de  $\mu\left(\frac{a}{b}\right)$  comme les sous-mots  $l...lc$  ou  $lc...c$ ; ces paliers se décrivent également par un rationnel mais notre définition conduit à une structure plus concise et à un algorithme plus rapidement convergent.

Exemple

Les mots de paliers associés aux rationnels  $\frac{7}{18}$  et  $\frac{11}{24}$  sont respectivement  $llclclc$  et  $lcccccccc$ . Dans le premier cas les paliers  $ll, l, l$  sont décrits

par les séquences montantes de la suite des restes du rationnel  $\frac{3}{4}$  (ie.0,3,2,1). Dans le deuxième les séquences montantes du rationnel  $\frac{2}{9}$  à savoir 0,2,4,6,8 et 1,3,5 7 décrivent bien les deux paliers cccc et cccc du mot de paliers.

## V LES BASES EUCLIDIENNES D'UN RESEAU ET LEURS APPLICATIONS

Dans ce paragraphe nous visons essentiellement deux choses, primo décrire, au moyen d'autres suites associées, l'ensemble des points d'une suite arithmétique  $\left\{\frac{ai}{b}\right\}$  contenus dans une fenêtre rectangulaire isothétique, cette question réapparaissant de façon réccurente en Géométrie Discrète, deuxio obtenir de nouveaux résultats de structure et algorithmes pour les droites discrètes. Il est commode pour cela de faire appel à la notion de réseau entier (ou sous-groupe de  $\mathbb{Z}^2$ ) courante en Géométrie des Nombres. C'est en leur associant une famille finie de bases remarquables, dites euclidiennes, liées à l'enveloppe convexe  $\mathcal{C}$  des points de la suite  $\left\{\frac{ai}{b}\right\}$  contenus dans le carré  $]0, b[{}^2$  que nous y parvenons.

Considérons le réseau plan associé à la suite des restes  $(i, \frac{ai}{b})$  prolongée par périodicité, c'est à dire le réseau engendré par les vecteurs  $(0, b)$  et  $(1, a)$ ; nous l'appellerons le réseau des restes du rationnel  $\frac{a}{b}$  et le désignerons par  $\mathcal{R}(\frac{a}{b})$ .

Par construction l'ensemble des points de  $\mathcal{R}(\frac{a}{b})$  contenus dans le carré  $]0, b-1[ \times ]0, b-1[$  est en bijection avec celui des points de la période de la droite naïve de pente  $\frac{a}{b}$ . Les séquences montantes, en correspondance avec les paliers de cette droite, sont toutes visibles sur cette partie du réseau.

### 1 L'algorithme de Jacobi-Perron et les bases euclidiennes d'un réseau entier

Rappelons l'algorithme de Jacobi-Perron bidimensionnel "entier", généralisation vectorielle de celui d'Euclide, (cf [42], [68], [102]).

Soient  $U_0 = (x_0, y_0)$  et  $U_1 = (x_1, y_1)$  deux vecteurs de  $\mathbb{Z}^2$  vérifiant les conditions:

$$\begin{aligned} x_0 \cdot x_1 < 0, \quad |x_0| < |x_1| & \quad (\alpha) \\ y_0 > y_1 \geq 0, \\ (y_0, y_1) = (x_0, x_1) = 1 \end{aligned}$$

Nous allons prolonger la suite  $U_i$  dans les deux sens. Traitons d'abord le cas  $i > 0$ . Supposons  $U_i = (x_i, y_i)$  défini pour  $i \geq 1$ , nous posons alors

$$U_{i+1} = U_{i-1} - q_i \cdot U_i$$

où  $q_i = \left[ \frac{y_{i-1}}{y_i} \right]$  est le quotient des deux dernières composantes en  $y$ . Par hypothèse les conditions  $(\alpha)$  sont encore vérifiées pour  $U_{i-1}$  et  $U_i$  et par construction elles seront prolongées à  $U_i$  et  $U_{i+1}$ . Si  $x_0 \leq 0$  et  $x_1 > 0$  tous les  $x_{2i}$  sont négatifs et les  $x_{2i+1}$  positifs avec un changement évident si  $x_0 \geq 0$ . Ces

relations induisent l'algorithme d'Euclide sur les composantes  $y_i$  et un algorithme de type "fraction continue" ou continuants sur les composantes  $x_i$ . Il est commode de regrouper la suite  $U_i$  dans un tableau comme suit

$x_i$	$x_0$	$x_1$	...	$x_{i-1}$	$x_i$	$x_{i-1} - q_i \cdot x_i$	...	$(-1)^p x_p$
$y_i$	$y_0$	$y_1$	...	$y_{i-1}$	$y_i$	$y_{i-1} - q_i \cdot y_i$	...	1

où nous avons supposé que la longueur de l'algorithme d'Euclide de la paire  $(y_0, y_1)$  est  $p$ .

Prolongeons aussi cette suite vectorielle dans l'autre direction en introduisant des vecteurs  $U_i$  pour  $i < 0$ . Nous supposons  $|x_0| < x_1$  et posons  $q_{-1} = \left[ \frac{x_1}{x_0} \right]$  ainsi que  $U_{-1} = U_1 + q_{-1} U_0$ . En supposant que  $U_{-1}$  soit défini et que l'on ait  $y_{-i} > y_{-i+1}$  et  $|x_{-i}| < |x_{-i+1}|$  nous définissons  $q_{-i-1} = \left[ \frac{|x_{-i+1}|}{|x_{-i}|} \right]$  et  $U_{-i-1} = U_{-i+1} + q_{-i-1} U_{-i}$ . Nous pouvons itérer cet algorithme jusqu'à ce que  $x_{-i}$  soit nul. Ce prolongement induit donc l'algorithme d'Euclide sur les  $x_i$ , c'est à dire sur la première ligne des matrices  $(U_{i-1}, U_i)$ . Notre pouvons donc considérer que l'algorithme de Jacobi-Perron est prolongé dans les deux sens.

Si nous posons  $\delta = |x_0 y_1 - x_1 y_0|$  il est facile de vérifier que la quantité  $x_i^{-1} y_i$  mod  $\delta$  reste invariante; en particulier elle est égale à  $x_0^{-1} y_0$  et à  $x_1^{-1} y_1$ ; nous pouvons donc la désigner par  $\varepsilon(U_0, U_1)$  ou par  $\varepsilon$  s'il n'y a pas d'ambiguïté. Aux deux extrémités de l'algorithme nous trouvons les couples de vecteurs  $\begin{pmatrix} 0 & 1 \\ \delta & \varepsilon \end{pmatrix}$  et  $\begin{pmatrix} \varepsilon^{-1} & (-1)^{p+1} \delta \\ 1 & 0 \end{pmatrix}$  où cette fois  $p$  est la longueur du développement en fraction continue du rationnel  $\frac{\varepsilon}{\delta}$ , le dernier quotient partiel, comme cela est toujours possible, étant égal à 1.

A tout couple  $(U_i, U_{i+1})$  de la suite précédente nous pouvons appliquer la transformation sur la première ligne ou sur la deuxième qui vont dans des directions opposées. Il est clair qu'en composant dans les deux sens nous obtenons la transformation identique. Par conséquent nous avons la

proposition 1

Deux couples de vecteurs  $(U_0, U_1)$  et  $(U'_0, U'_1)$  vérifiant les conditions  $(\alpha)$  appartiennent à la même suite de Jacobi-Perron si et seulement si ils ont

mêmes déterminants (au signe près) et mêmes constantes  $\varepsilon$ .

Introduisons, sous l'hypothèse  $(\alpha)$ , l'extension additive de l'algorithme vectoriel précédent i.e. nous posons  $V_{i,0} = U_i$  pour  $i=0,1,\dots,p$  et  $i$  étant choisi dans l'intervalle précédent on pose pour  $j=0,1,2,\dots,q_{i+1}-1$

$$V_{i,j} = U_i^{-j} \cdot U_{i+1}$$

et pour  $j=q_{i+1}$

$$V_{i+2,0} = U_{i+2} = U_i^{-q_{i+1}} \cdot U_{i+1}$$

La suite  $V_{0,0}, V_{0,1}, \dots, V_{0,q_1-1}, V_{1,0}, V_{1,1}, \dots$  est la forme additive de l'algorithme vectoriel précédent. Si nous désignons par  $(\Sigma_p)$  (resp.  $(\Sigma_i)$ ) la sous-suite de la précédente dont le premier indice  $i$  est pair (resp. impair) et par  $\delta$  la constante entière  $\det(U_1, U_0)$ , nous avons la propriété suivante.

### proposition 2

a) Si  $V$  et  $V'$  sont deux vecteurs consécutifs de la suite  $(\Sigma_p)$   $\det(V, V') = \delta$ ;  
si  $V$  et  $V'$  sont deux vecteurs consécutifs de la suite  $(\Sigma_i)$   $\det(V, V') = -\delta$ .

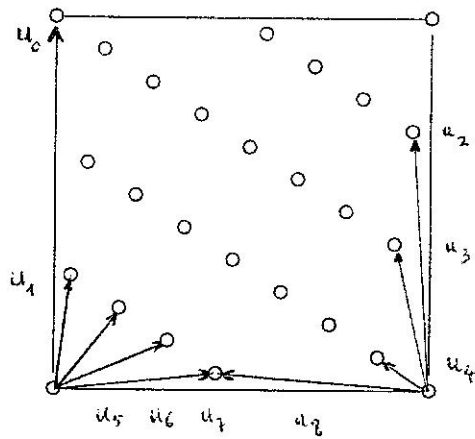
b) Les couples de vecteurs consécutifs de la suite  $(\Sigma_p)$  ou de la suite  $(\Sigma_i)$  sont des bases du réseau engendré par  $U_0$  et  $U_1$ .

Soit  $\mathcal{R}(U_0, U_1)$  un réseau entier (sous-groupe additif de  $\mathbb{Z}^2$ ) pour lequel on a  $(x_0, x_1) = (y_0, y_1) = (x_0, y_0) = 1$ . Ses bases euclidiennes sont les couples de vecteurs consécutifs des suites  $(\Sigma_p)$  et  $(\Sigma_i)$  associées à l'algorithme de Jacobi-Perron additif engendré par  $\begin{pmatrix} 0 & 1 \\ \delta & \varepsilon \end{pmatrix}$ ;  $\delta$  étant  $|x_0 y_1 - x_1 y_0|$  et  $\varepsilon = x_0^{-1} y_0 \pmod{\delta}$ .

Le réseau  $\mathcal{R}(U_0, U_1)$  coïncide avec le réseau des restes  $\mathcal{R}(\frac{\varepsilon}{\delta})$ ; nous en déduisons la proposition ci-dessous.

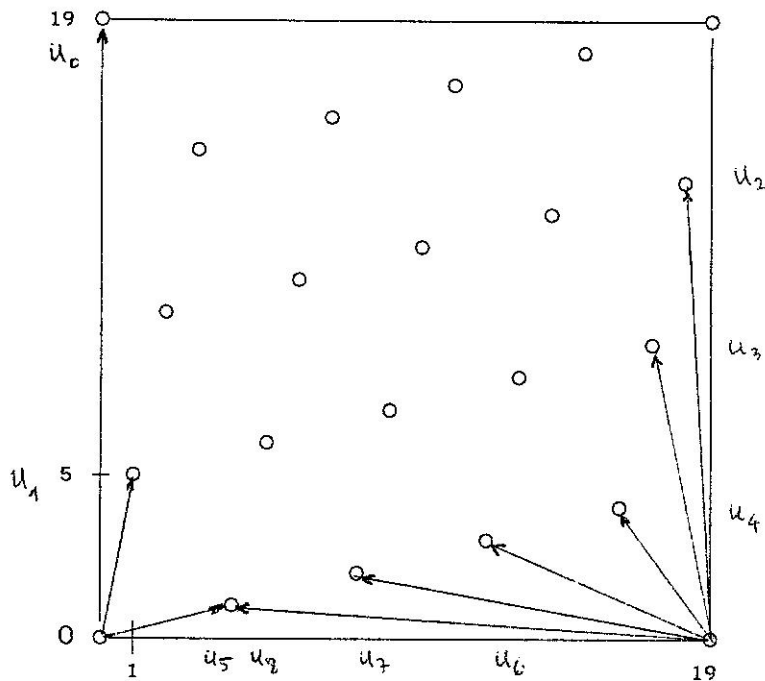
### proposition 3

Soit  $\mathcal{R}$  un réseau entier et  $(U_0, U_1)$  une de ses bases, alors elle appartient à la famille des bases euclidiennes de  $\mathcal{R}$  si et seulement si elle vérifie les conditions  $x_0 x_1 \geq 0$ ,  $y_0 > 0$ ,  $y_1 > 0$  et  $(x_1 - x_0)(y_1 - y_0) \leq 0$ .



Les bases euclidiennes d'un réseau entier

La suite  $U_i$  pour le rationnel  $\frac{a}{b} = \frac{7}{23}$



Les bases euclidiennes d'un réseau entier.

La suite  $U_i$  pour le rationnel  $\frac{a}{b} = \frac{5}{19}$ .

figure 1

## 2 Une généralisation du diagramme de Klein aux réseaux entiers.

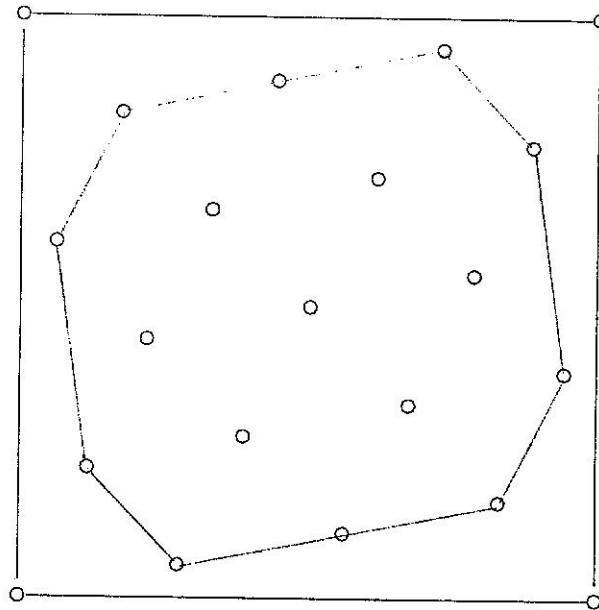
Un réseau entier  $\mathcal{R}$  étant donné, considérons la suite  $W_0, W_1, \dots$  des vecteurs de  $(\Sigma_p)$ ; nous pouvons supposer que ceux-ci ont leurs composantes positives ou nulles et que  $W_0 = (0, \delta)$  et  $W_1 = (1, \varepsilon)$ . Il résulte du § précédent que la suite des pentes des vecteurs  $W_{i+1} - W_i$  est décroissante (ce sont des vecteurs de la suite  $(\Sigma_i)$ ) autrement dit que la ligne polygonale issue du point  $(0, \delta)$  passant par les extrémités des vecteurs  $W_0, W_1, W_2, \dots$  est

convexe.

Remarque La ligne polygonale envisagée (tracée dans  $\mathbb{R}^2 \supset \mathbb{Z}^2$ ) ne signifie pas que nous ayons recours à une notion continue; c'est une façon commode à la fois de définir des suites discrètes et de les représenter graphiquement. Ceci s'appliquera chaque fois que nous parlerons de lignes polygonales ou d'enveloppes convexes.

En considérant la suite analogue associée aux vecteurs de la suite  $(\Sigma_i)$  nous voyons que la ligne polygonale également issue de  $(0, \delta)$  et passant par les extrémités de ces derniers est aussi convexe. Comme  $\mathcal{R}$  est doublement périodique dans les directions  $x$  et  $y$  et de période  $\delta$  nous en déduisons, à condition d'interpréter les termes négatifs modulo  $\delta$ , que les vecteurs de l'algorithme de Jacobi-Perron décrivent l'enveloppe convexe des points de  $\mathcal{R}$  contenus dans le carré  $]0, \delta[x]0, \delta[$ . La symétrie par rapport à l'origine du réseau  $\mathcal{R}$  induit une symétrie de l'enveloppe convexe par rapport au centre du carré  $]0, \delta[x]0, \delta[$ . Par construction nous voyons que les sommets de cette enveloppe convexe sont donnés par l'algorithme de Jacobi-Perron multiplicatif alors que les points entiers situés sur cette enveloppe convexe sont décrits par la version additive de ce dernier.

Cette propriété de convexité de la suite arithmétique  $\{\frac{\epsilon_i}{\delta}\}$  est à rapprocher du théorème de convexité de Klein (cf [29], [53], [116]) pour le rationnel  $\frac{\epsilon}{\delta}$ .



L'enveloppe convexe et la suite des  
du rationnel  $\frac{11}{18}$ .

fig. 2

Exemple.

Prenons le réseau entier de constantes  $\delta=31$  et  $\varepsilon=18$ ; l'algorithme de Jacobi-Perron donne la suite de vecteurs contenue dans le tableau suivant:

$x_i$	0	1	-1	2	-5	7	-12	19	-31
$y_i$	31	18	13	5	3	2	1	1	0

duquel nous déduisons les coordonnées des sommets de l'enveloppe convexe des points de  $\mathcal{R}$  contenus dans le carré  $]0,31[x]0,31[$ . En commençant par (1,18) et en parcourant l'enveloppe dans le sens direct cette liste est:

(1,18), (2,5), (7,2), (19,1), (26,3), (30,13), (29,26), (24,29), (12,30), (5,28).

La version additive de l'algorithme ferait apparaître les nouveaux points (3,23) et (28,8).

La relation établie entre le réseau entier  $\mathcal{R}(U_0, U_1)$ , le réseau des restes  $\mathcal{R}(\frac{\varepsilon}{\delta})$  et le développement en fraction continue de  $\frac{\varepsilon}{\delta}=[0; q_1, q_2, \dots, q_n]$  permet d'évaluer les nombres de sommets (donc de côtés) et de points de  $\mathcal{R}$  situés sur l'enveloppe convexe  $\mathcal{C}$ .

### Théorème 1

- a) L'enveloppe convexe  $\mathcal{C}$  possède  $2n$  sommets (et  $2n$  côtés).
- b) On trouve  $2(\sum_{i=1}^n q_i - 2)$  points de  $\mathcal{R}$  sur  $\mathcal{C}$ .

### 3 Quelques inégalités modulaires

Les propriétés de convexité dégagées au § précédent vont nous permettre d'établir quelques inéquations modulaires du type

$$aX + b \left\langle \frac{\varepsilon X}{\delta} \right\rangle \geq \delta$$

et

$$aX + b \left\langle \frac{\varepsilon X}{\delta} \right\rangle \leq \delta$$

où  $\varepsilon$  et  $\delta$  sont deux entiers donnés et pour lesquelles nous cherchons à déterminer deux constantes entières  $a$  et  $b$  pour que ces inéquations soient identiquement vérifiées lorsque  $X$  parcourt l'intervalle  $]0, \delta[$  de  $\mathbb{N}$ .

L'étude de l'enveloppe convexe précédente nous donne immédiatement le résultat suivant après écriture des équations des droites qui bordent ce convexe.

### Théorème 2

Si  $\{U_i\}_{i>0}$  désigne la suite de Jacobi-Perron multiplicative induite par les vecteurs  $(0, \delta)$  et  $(1, \varepsilon)$  où  $U_i = (x_i, y_i)$  alors

$$\forall X \in ]0, \delta[ \text{ on a } y_i X - x_i \left\langle \frac{\varepsilon X}{\delta} \right\rangle \begin{cases} \geq \delta & \text{si } i \text{ est impair} \\ \leq \delta & \text{si } i \text{ est pair} \end{cases}$$

### Exemple

Si nous prenons  $\varepsilon=18$  et  $\delta=31$  la suite des vecteurs  $U_i$  est donnée par le tableau précédent. Avec  $i=2$  nous obtenons l'inégalité

$$\forall X \in ]0, 31[ \text{ on a } 13X + \left\langle \frac{18X}{31} \right\rangle \geq 31$$

tandis que  $i=5$  nous donne

$$\forall X \in ]0, 31[ \text{ on a } 2X - 7 \left\langle \frac{18X}{31} \right\rangle \leq 31.$$

Ces inéquations sont à rapprocher de la technique des "coupures de Gomory" utilisées en Programmation Entière. Si nous cherchons à déterminer les points entiers d'un convexe réel donné  $C$  elles permettent d'élaguer peu à peu quelques morceaux de  $C$  tout en maintenant la convexité jusqu'à faire apparaître un point entier sur le bord. L'analogie avec notre problème est claire; ici le rôle de  $C$  est joué par le carré des périodes  $[0, \delta]^2$  dans lequel

nous cherchons les autres points du réseau; notre enveloppe convexe érode ce qu'il faut pour les faire apparaître sur le bord. Il serait peut-être intéressant de voir si cette approche arithmétique se laisse généraliser à des situations plus représentatives de celles que l'on rencontre en Programmation Entière.

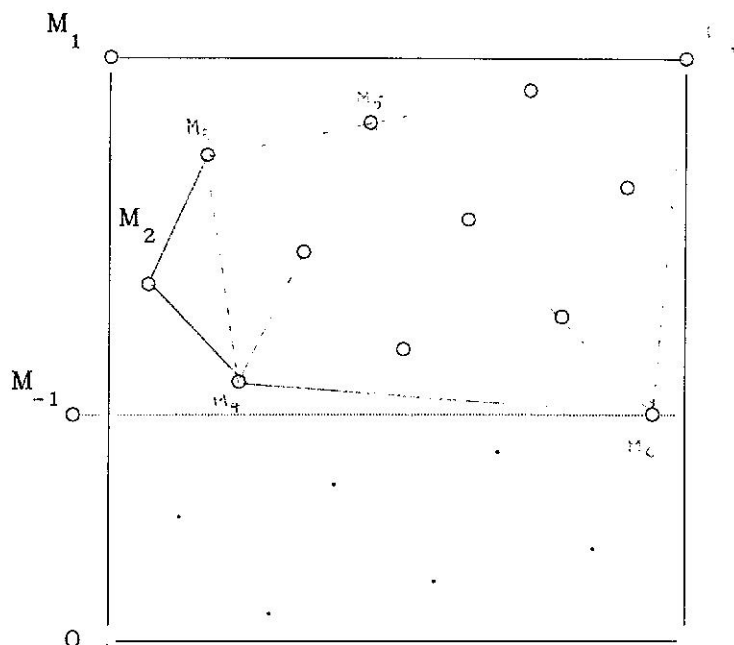
#### 4 Les bases euclidiennes et les droites discrètes; nouveau tracé.

Précisons maintenant un peu plus leur rôle pour les droites discrètes:

- o La liaison qu'elles établissent entre les points du réseau des restes et l'enveloppe convexe  $\mathcal{C}$ , permet de décrire d'autres enveloppes convexes et amène de nouveaux théorèmes de structure pour la droite associée.
- o Elles introduisent une suite de valeurs critiques qui délimitent les domaines de validité des paramétrages canoniques des points du réseau des restes contenus dans des fenêtres isothétiques.
- o Elles sont liées aux minima successifs du réseau et contrôlent par là les propriétés générales d'intersection des droites discrètes.

Pour l'instant nous allons examiner le premier point; les deux autres feront l'objet des paragraphes suivants.

Nous savons (IV prop. 1) que les fins de paliers de la droite de pente  $\frac{a}{b}$  correspondent aux valeurs de la suite des restes supérieures ou égales à  $b-a$  et que cette valeur est atteinte en  $i=b-1$ . Par conséquent les points de  $\mathcal{R}(\frac{a}{b})$  contenus  $[0, b-1]^2$  qui correspondent aux fins de paliers appartiennent au rectangle  $[0, b] \times [b-a, b]$ . Nous pouvons alors considérer l'enveloppe convexe  $\Phi$  des points de  $\mathcal{R}$  contenus dans  $[0, b] \times [b-a, b]$  et la suite obtenue en triant selon les abscisses croissantes les éléments de  $\mathcal{R}$  contenus dans  $\Phi$  ce qui revient à introduire la ligne polygonale  $\Gamma$  qui relie ces points. La figure suivante illustre ces deux courbes.



L'enveloppe convexe des fins de paliers  
du rationnel  $\frac{11}{18}$ .

fig. 3

La ligne  $\Gamma$  rencontre et rebondit sur  $\Phi$  aux points que nous notons  $M_2, M_3, \dots, M_n$ . Il est clair que la partie supérieure de l'enveloppe convexe  $\Phi$  coïncide avec celle de  $\mathcal{C}$  et que la partie inférieure est la translaturée, (de vecteur  $(-1,0)$ ), de la partie inférieure de  $\mathcal{C}$ . D'après le théorème 1 précédent l'entier  $n$  est la longueur de l'algorithme d'Euclide du couple  $(a,b)$  ie tel que  $\frac{a}{b} = [0; q_1, q_2, \dots, q_n]$ . Posons  $M_{-1} = (-1, b-a)$  et  $M_1 = (0, b)$  qui appartiennent à  $\mathcal{R}$ ; Désignons par  $\Gamma_i(M_{-1})$ , (resp.  $\Gamma_i(M_1)$ ) la partie de la ligne polygonale  $\Gamma$  joignant  $M_2$  à  $M_i$  préfixée du segment  $M_{-1}M_2$  (resp.  $M_1M_2$ ). Par conséquent  $\Gamma_i(M_{-1}) = M_{-1}M_2M_3 \dots M_i$  et  $\Gamma_i(M_1) = M_1M_2M_3 \dots M_i$ .

### théorème 3

Avec les notations précédentes on a pour tout  $i \in [2, n-1]$  la relation de récurrence

$$\Gamma_{i+1}^{(-)}(M_{i+1}) = q_{i+1} \Gamma_i^{(-)}(M_{i+1}) + \Gamma_{i-1}^{(-)}(M_{i+1})$$

où l'expression  $q\Gamma$  désigne la concaténation de  $q$  exemplaires de  $\Gamma$  mis bout à bout.

Sur l'exemple précédent  $\frac{21}{34} = [11111111]$  nous voyons en particulier que  $\Gamma_6 = \Gamma_5(M_1) + \Gamma_4(M_1)$ .

En projetant sur l'axe des  $x$  et en désignant par  $X_i, i \in [2, n]$ , l'ensemble des abscisses des fins de paliers inférieures à l'abscisse de  $M_1$  nous obtenons un algorithme qui permet de calculer les abscisses des fins de palier d'une droite naïve de pente  $\frac{a}{b}$  en  $\sim \log(a)$  opérations; chacune d'elle est une translation d'un ensemble fini de valeurs. Cet algorithme fait moins d'opérations que l'algorithme des fins de paliers, du §IV 3 fondé sur la suite  $\left\{ \frac{(a - \frac{b}{a})i}{a} \right\}$  et de plus il élimine toutes les comparaisons que celui-ci réclamait. Cet algorithme extrait à chaque étape le quotient partiel  $q_i$  nécessaire.

Désignons par  $\{r_i\}$  la suite des restes de l'algorithme d'Euclide de  $a$  et  $b$  parcourue à l'envers, à savoir la suite définie par

$$r_{-1} = 0, r_0 = 1, \text{ et } \forall i > 0 \quad r_i = q_i r_{i-1} + r_{i-2}$$

Notons  $\tilde{X}_i$  le perturbé de l'ensemble  $X_i$  défini comme ci-dessous

$$\tilde{X}_i = \begin{cases} X_i & \text{si } i \text{ pair} \\ X_i \setminus \{s_i\} \cup \{s_i + 1\} & \text{si } i \text{ impair} \end{cases}$$

où  $s_i$  désigne le plus grand élément de  $X_i$  et  $\setminus$  la différence ensembliste (en fait  $s_i = r_{i-1}$ ). Autrement dit  $\tilde{X}_i$  est obtenu à partir de  $X_i$  en augmentant d'une unité son plus grand élément lorsque  $i$  est impair (c'est l'influence du changement de préfixe contenu dans le théorème précédent). Sur les  $X_i$  (et  $\tilde{X}_i$ ) le théorème se traduit par la relation de récurrence suivante:

$$X_0 = \emptyset, X_1 = \{q_1 - 1\}, \text{ et } \forall i > 0 \quad X_{i+1} = \bigcup_{0 \leq k < q_{i+1}} (\tilde{X}_i + k r_i) \cup (X_{i-1} + q_{i+1} r_i)$$

qui constitue l'algorithme des fins de palier par convexité.

Pratiquement nous disposons les quotients partiels, les  $r_i$ , les  $X_i$  dans trois colonnes consécutives comme dans l'exemple suivant.

Exemple:  $\frac{a}{b} = \frac{31}{49} = [0;1,1,1,2,1,1,2]$

i	q <sub>i</sub>	r <sub>i</sub>	X <sub>i</sub>
0		1	∅
1	1	1	0
2	1	2	1
3	1	3	1 2
4	2	8	1 3 4 6 7
5	1	11	1 3 4 6 7 9 10
6	1	19	1 3 4 6 7 9 11 12 14 15 17 18
7	2	49	1 3 4 6 7 9 11 12 14 15 17 18 20 22 23 25 26 28 30 31 33 34 36 37 39 41 42 44 45 47 48

Cet exemple révèle la simplicité et la rapidité de cet algorithme.

### 5 Le parcours des points d'un réseau dans un rectangle isothétique

Soit  $\frac{a}{b}$  un rationnel vérifiant comme ci-dessus les conditions  $0 < a < b$  et  $(a,b)=1$ ,  $\mathcal{R}$  le réseau des restes associé et  $F(h)$  la fenêtre rectangulaire  $[0,b[x[0,h[$  où  $h \in [0,b-1[$ . Convenons d'appeler parcours canonique des points de  $\mathcal{R} \cap F(h)$  celui qui les rencontre dans l'ordre croissant de leurs abscisses; il est bien défini puisque  $0 \leq h < b$ . Soient,  $U=(\kappa,\gamma)$  et  $U'=(\kappa',\gamma')$  les deux vecteurs de l'algorithme de Jacobi-Perron additif engendré à partir de  $(0,b)$  et  $(1,a)$  qui vérifient les conditions

$$\gamma' \geq h > \gamma.$$

Nous définissons les deux vecteurs  $A=(\alpha,\beta)$  et  $A'=(\alpha',\beta')$  par les relations

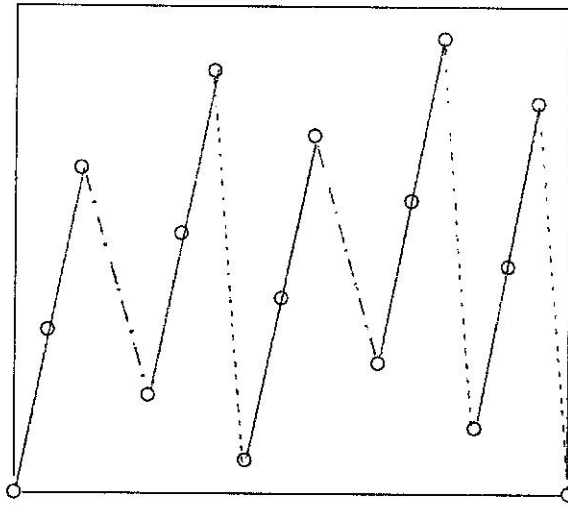
$$A=U, A'=U-U' \text{ si } \kappa > 0$$

et

$$A=U'-U, A'=-U \text{ si } \kappa < 0.$$

L'algorithme suivant, dit des "3 vecteurs"  $A$ ,  $A'$  et  $A+A'$ , contrôlé par le rationnel  $\frac{\beta}{\gamma}$ , effectue le parcours canonique cherché. Le point courant de cette suite de  $\mathcal{R} \cap F(h)$  y est désigné par  $X=(x,y)$ .

<p>Algorithme des trois vecteurs</p> <pre> X=0; r=0; for i=1 to h-1 do     if r &lt; h-β then begin r=r+β;      X=X+A      end     else if r &lt; γ'-β then begin r=r+2β-γ'; X=X+2A-A' end     else begin r=r+β-γ'; X=X+A-A' end; </pre>
--



Les 3 vecteurs associés à une fenêtre  $F(h)$ .

Rationnel  $\frac{5}{17}$ , hauteur 15.

Fig.4

Remarque.

Cet algorithme, qui permet d'effectuer le parcours canonique de  $\mathcal{R} \cap F(h)$ , peut dans certaines circonstances, (si la hauteur  $h$  est euclidienne; cf. § suivant), être décrit par des suites arithmétiques. Par contre si la hauteur n'est plus euclidienne la description par formules analytiques de ce parcours se complique énormément. L'élément perturbateur ici est l'algorithme d'Euclide derrière le convexe  $\mathcal{C}$ ; il modifie, parfois peu, parfois beaucoup, la simplicité de la suite arithmétique  $\left\{ \frac{ax}{b} \right\}$ . Nous précisons ce "beaucoup" au §IX.

La connaissance du nombre de points du réseau dans  $F(h)=[0,b[x[0,h[$ , i.e.  $h$  nous permet de les indexer par  $i \in [0, h-1[$ . Par contre si la largeur de la fenêtre change, par exemple si nous nous intéressons aux points du réseau contenus dans  $[0,k[x[0,h[$  où  $h$  et  $k \in [0, b-1[$  on ne sait pas encore trouver le nombre de points contenus; il faut introduire un contrôle sur l'abscisse des points celle-ci, contenue dans  $x$  étant connue à tout moment.

Par division euclidienne une fenêtre isothétique quelconque se décompose en un nombre fini de fenêtres carrées  $[0, b]^2$  et de fenêtres pdu type précédent.

Examinons comment ce parcours est modifié lorsque la fenêtre  $F(h)$  se déplace sur le réseau; désignons maintenant par  $F(h)'$  la fenêtre  $[x_0, x_0 + b] \times [y_0, y_0 + h]$  où  $(x_0, y_0)$  est un point entier quelconque et  $h$  comme ci-dessus. Nous savons, par périodicité, que la suite associée au parcours canonique dans cette fenêtre, est une translatée de la précédente. La mise en accord entre elles se fait en calculant l'abscisse du point d'ordonnée  $y_0$  situé sur le bord inférieur de  $F(h)'$ . L'abscisse de ce point est  $x_1 = x_0 + \left\{ \frac{y_0 \cdot a^{-1} - x_0}{b} \right\}$  (où  $a^{-1} \in [1, b-1]$  est calculé mod  $b$ ). En initialisant  $X$  à  $(x_1, y_0)$  et en parcourant la suite d'abord vers la droite tant que  $x < x_0 + b$ , puis vers la gauche tant que  $x > x_0$ , nous obtenons le cheminement désiré.

Dans certaines circonstances (si la largeur de la fenêtre est  $< a^{-1}$  par exemple) il est souhaitable de commencer le parcours à partir du point  $M$  de  $\mathcal{R} \cap F(h)'$  d'abscisse minimale. Remarquons bien que cette contrainte impose à priori de connaître deux nouveaux éléments: l'indice  $i_0$  de  $M$  dans la suite canonique (liée à  $\mathcal{R} \cap F(h)$ ), celui-ci étant bien défini et le décalage de  $M$  par rapport au bord gauche de la fenêtre,  $\phi = \text{abscisse}(M) - x_0$ . Or leur détermination, c'est à dire la recherche de formules qui les évalue n'est pas simple; nous procédons différemment, en suivant un peu l'algorithme de Perron-Jacobi, pour définir  $M$ . Si la hauteur  $h$  est "euclidienne" les deux quantités mentionnées se calculent bien; ce sera fait au paragraphe suivant.

Il est clair que le point  $(x_0, y_0 - \left\{ \frac{ax_0}{b} \right\})$  est le point du réseau des restes d'abscisse  $x_0$  et situé immédiatement en dessous du coin inférieur gauche  $(x_0, y_0)$  de la fenêtre. En appliquant aux vecteurs  $(0, b)$  et  $(1, a)$ , repérés à partir de cette nouvelle origine, l'algorithme de Jacobi-Perron tant que la deuxième composante du vecteur courant est supérieure à  $h + \left\{ \frac{ax_0}{b} \right\}$  nous trouvons, à la sortie, le point  $M$ . Ceci se formalise comme suit.

```

Algorithmme du premier point
u0=0; v0=b;
u1=1; v1=a;

seuil=h+ $\left\{\frac{y_0 - \left(\frac{ax_0}{b}\right)}{b}\right\}$ 

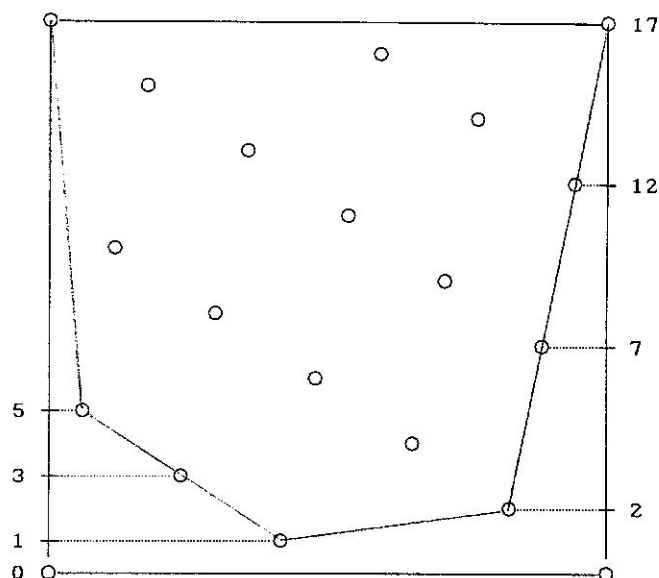
If seuil ≥ v0 then premier_point=(u0,v0)
else if seuil ≥ v1 then premier_point=(u1,v1)
else while seuil < y1 repeat
begin
u = u0 -  $\left[\frac{v_0}{v_1}\right] u_1$ ; u0 = u1; u1 = u;
v =  $\left\{\frac{v_0}{v_1}\right\}$ ; v0 = v1; v1 = v;
end;
premier_point=(u1,v1);

```

Il va sans dire que si un même réseau doit être parcouru par de nombreuses fenêtres il est plus efficace de stocker la suite des hauteurs euclidiennes et de comparer la valeur seuil aux termes de cette liste.

### 6 Le paramétrage des points d'un réseau dans une fenêtre euclidienne

Le paragraphe précédent montre que nous pouvons décrire algorithmiquement les points d'un réseau entier dans toute fenêtre isothétique  $F(h)=[0,b] \times [0,h]$  ou plus généralement de la forme  $[x_0, x_0+b] \times [y_0, y_0+h]$ ; or dans certaines (par exemple  $[0,b] \times [0,b]$ ) nous pouvons paramétrer l'ensemble par une suite arithmétique (comme  $(i, \frac{ai}{b})$ ). Il est légitime de se demander s'il est possible de trouver un paramétrage, éventuellement un peu plus compliqué puisque les ensembles n'ont pas les mêmes structures, dans toutes les fenêtres. Ce problème est assez difficile dans le cas général mais il admet des solutions simples lorsque les hauteurs des fenêtres sont "euclidiennes" i.e. égales à la deuxième composante de l'un des vecteurs  $U_i$  définis par les points du réseau des restes situés sur l'enveloppe convexe  $\mathcal{C}^*_i$  de ceux contenus dans  $[0,b] \times [1,b]$  (voir fig. ??? suivante). Soit  $U=(\xi, \eta)$  le point de cette enveloppe convexe dont l'ordonnée  $\eta < h$  est la plus grande possible. Nous pouvons supposer, qui à échanger des noms de vecteurs que  $\xi > 0$ ; nous dirons que  $U$  est le générateur de la fenêtre.



Le convexe donnant les hauteurs des  
fenêtres euclidiennes du rationnel  $\frac{5}{17}$ .

Fig. 5

D'après la définition de l'algorithme des 3 vecteurs il est clair que celui-ci se réduit à un tracé naïf si et seulement si  $h$  vérifie l'une des conditions

$$h=\eta \text{ ou}$$

$$h=\eta' \text{ ou}$$

$$h=\eta'-\eta.$$

Ceci donne immédiatement

#### proposition 4

*Les valeurs de  $h$  pour lesquelles l'algorithme des 3-vecteurs se réduit à un tracé naïf sont les ordonnées des points du réseau situés sur l'enveloppe convexe  $\mathcal{C}^*$ ; i.e. les fenêtres euclidiennes sont celles qui passent par les points du réseau situés sur  $\mathcal{C}^*$ .*

Si  $F(h)$  est une fenêtre euclidienne de générateur  $U(\xi, \eta)$  alors

#### proposition 5

*Les points du réseau contenus dans  $F(h)=[0,b] \times [0,h[$  sont donnés par la suite*

$$\begin{cases} x(i) = \xi i + \left( \frac{b-h\xi}{\eta} \right) \left[ \frac{\eta i}{h} \right] \\ y(i) = \left\{ \frac{\eta i}{h} \right\} \end{cases} \quad \text{pour } i=0,1,\dots,h-1.$$

remarque: la constante  $\frac{b-h\xi}{\eta}$  est un entier et non pas un rationnel.

Si  $\frac{a}{b} = [0; q_1, q_2, \dots, q_n]$  les hauteurs des fenêtres euclidiennes, c'est à dire les ordonnées des point du réseau des restes situés sur la courbe convexe  $\mathcal{C}^*$ , sont déterminées par la suite

$$H_{i,j} = jK_i(q_{n-i+1}, \dots, q_n) + K_{i-1}(q_{n-i+2}, \dots, q_n),$$

où  $i \in [0, \dots, n-1]$ ,  $j \in [1, \dots, q_{n-i}]$  et, par convention  $K_{-1} = 0$ .

Exemple Si  $\frac{a}{b} = \frac{181}{341} = [0; 2, 2, 3, 2, 3, 3]$  les hauteurs  $H_{i,j}$  s'obtiennent en prolongeant de façon canonique l'algorithme de calcul du rationnel associé à un développement en fraction continue:

$j \setminus i$	0	1	2	3	4	5	6
0	341	181	79	23	10	3	1
1		260	102	33	13	4	2
2				56		7	
3							
$q_i$		2	2	3	2	3	3

Algorithme des hauteurs euclidiennes

La ligne  $j=0$  correspond à l'algorithme d'Euclide de (341,181) dans un sens et à l'algorithme de calcul du rationnel  $\frac{181}{341}$  à partir de son développement en fraction continue dans l'autre. Les lignes  $j>0$  contiennent les valeurs de l'algorithme d'Euclide "soustractif" de ce couple d'entiers.

Donnons maintenant la formule de paramétrage complète valable lorsque la fenêtre se déplace verticalement, i.e. lorsqu'elle est de la forme  $[0, b] \times [y_0, y_0 + h]$ , avec  $y_0 \neq kb$ . La situation sera la même qu'avec  $y_0 = kb$  à un décalage près que nous explicitons.

Nous introduisons  $a^{-1} \pmod b$  et  $\eta^{-1} \pmod h$  que nous notons, pour simplifier  $a^{-1}$  et  $\eta^{-1}$ ; puis  $i_0 = \left\{ \frac{y_0 \eta^{-1}}{h} \right\} + \left[ \frac{y_0 + h - 1}{b} \right] - \left[ \frac{y_0}{b} \right]$  et  $x_0 = \left\{ \frac{y_0 a^{-1}}{b} \right\}$  alors le paramétrage des points du réseau dans la fenêtre  $[0, b] \times [y_0, y_0 + h]$  s'écrit

$$\begin{cases} x(i) = \xi(i - i_0) + \left( \frac{b - h\xi}{\eta} \right) \left[ \frac{\eta(i - i_0)}{h} \right] + x_0 \\ y(i) = \left\{ \frac{\eta(i - i_0)}{h} \right\} + y_0 \end{cases} \quad \text{pour } i=0, 1, \dots, h-1.$$

### 7 La résolution des inéquations modulaires

Pour un couple d'entiers  $a$  et  $b$  vérifiant toujours les mêmes conditions, à savoir  $0 < a < b$  et  $(a, b) = 1$  nous sommes parfois amenés à rechercher les solutions de l'inégalité

$$0 \leq \left\{ \frac{ax}{b} \right\} < k$$

où  $k$  est une constante entière inférieure à  $b$ . Nous qualifions de modulaire une telle inéquation.

D'après le §6 ci-dessus nous savons la résoudre si  $c$  est l'une des hauteurs euclidiennes du couple  $(a, b)$  puisque nous savons paramétrer l'ensemble des points du réseau des restes dans une fenêtre euclidienne. Dans le cas général nous pouvons décomposer l'entier  $k$  en somme de valeurs euclidiennes puis décomposer la fenêtre  $[0, b] \times [0, k]$  en fenêtres horizontales ayant ces hauteurs. Nous pouvons ainsi décomposer l'ensemble des solutions en réunion de plusieurs ensembles que nous pouvons paramétrer explicitement au moyen des formules du § précédent.

## VI LES MINIMA DU RESEAU DES RESTES

### 1 Enveloppe convexe et continuants de FANTET DE LAGNY

Nous désignons par  $K_p(x_1, x_2, x_3, \dots, x_p)$  le polynôme formé de la somme de tous les monômes obtenus à partir du produit  $x_1 x_2 x_3 \dots x_p$  en éliminant les paires  $x_k x_{k+1}$  de toutes les façons possibles. Si  $p$  est pair l'un de ces monômes, égal à 1, résulte de l'élimination de toutes les variables. Les premiers  $K_p$  sont alors

$$\begin{aligned} K_0 &= 1, \\ K_1(x_1) &= x_1, \\ K_2(x_1, x_2) &= x_1 x_2 + 1, \\ K_3(x_1, x_2, x_3) &= x_1 x_2 x_3 + x_1 + x_3, \\ K_4(x_1, x_2, x_3, x_4) &= x_1 x_2 x_3 x_4 + x_1 x_2 + x_1 x_4 + x_3 x_4 + 1. \end{aligned}$$

Nous savons que les  $K_p$ , continuants de Fantey de Lagny (souvent attribués à Euler) expriment le numérateur et le dénominateur d'une fraction continue de quotients partiels connus.

On a la relation

$$[q_0; q_1, q_2, q_3, \dots, q_n] = \frac{K_{n+1}(q_0, q_1, \dots, q_n)}{K_n(q_1, q_2, \dots, q_n)}$$

(Voir [47] pour une présentation limpide des propriétés de ces polynômes).

La relation précédente montre que les continuants expriment tous les termes de la suite engendrée par l'algorithme d'Euclide d'un rationnel  $\frac{a}{b}$  en fonction de ses quotients partiels. De même les composantes de l'algorithme de Jacobi-Perron engendré par les vecteurs  $U_0 = (0, \delta)$  et  $U_1 = (1, \varepsilon)$  s'écrivent avec les continuants du couple  $(\delta, \varepsilon)$ . Nous pouvons en déduire les coordonnées des sommets de l'enveloppe convexe des points du réseau engendré par ces deux vecteurs dans  $]0, \delta[^2$  et par là les minima du réseau. Le résultat suivant est immédiat.

#### proposition 1

Supposons que  $\frac{\varepsilon}{\delta} = [0; q_1, q_2, q_3, \dots, q_n, 1]$  alors les coordonnées des sommets de la partie inférieure de l'enveloppe convexe sont donnés par les formules suivantes:

$$\begin{cases} x_k = (-1)^{k-1} K_{k-1}(q_1, q_2, \dots, q_{k-1}) \\ y_k = K_{n-k}(q_{k+1}, \dots, q_n, 1) \end{cases}$$

pour  $k=1, 2, \dots, n$ .

Les points de la partie supérieure sont les  $(b-x_k, b-y_k)$ ,  $k=1, \dots, n$ .

## 2 Les vecteurs minimaux du réseau des restes

Nous supposons dans ce § que nous avons un réseau vérifiant les hypothèses (α) ie qu'il est engendré par deux vecteurs  $U_0=(0,\delta)$  et  $U_1=(1,\varepsilon)$  avec  $0<\varepsilon<\delta$  et  $(\varepsilon,\delta)=1$ . Ce réseau est donc engendré par la suite des restes d'une droite discrète de pente  $\frac{\varepsilon}{\delta}$ . Nous nous intéressons alors à une base minimale de celui-ci; les bases minimales intervenant dans l'intersection des droites discrètes.

Pour résoudre ce problème il suffit de chercher les points de l'enveloppe convexe inférieure les plus voisins de l'origine et du point  $(\delta,0)$  (ie l'origine modulo  $\delta$ ). Autrement dit nous cherchons à résoudre le problème d'optimisation suivant

$$\text{Min}_{1 \leq i \leq n} K_i(q_1, \dots, q_{i-1})^2 + K_{n-i}(q_{i+1}, \dots, q_n, 1)^2$$

Si nous désignons encore par  $U_i = (x_i, y_i)$  les vecteurs de la suite de Jacobi-Perron multiplicative engendrés par  $U_0$  et  $U_1$ , tout revient à trouver l'indice  $i_0$  du minimum de

$$s_i^2 = x_i^2 + y_i^2$$

La suite des  $|x_i|$  est croissante de 0 à  $\delta$  tandis que les  $y_i$  décroissent de  $\delta$  à 0. Nous allons montrer que le minimum cherché est donné par l'indice de croisement de ces deux suites. Plus précisément soit  $i_c$  l'indice entier vérifiant

$$y_{i_c} \geq |x_{i_c}| \text{ et } y_{i_c+1} < |x_{i_c+1}|$$

Nous avons la

### proposition 2

*Le sommet de  $\mathcal{C}$  le plus proche de l'origine est l'un des vecteurs  $U_i$ , où  $i \in \{i_c-1, i_c, i_c+1, i_c+2\}$ .*

Par conséquent les points de  $\mathcal{C}$  les plus proches de  $(0,0)$  ou de  $(b,0)$  se déterminent en comparant les longueurs des côtés des deux triangles construits sur  $U_{i_c-1}$  et  $U_{i_c}$  d'une part et  $U_{i_c+1}$ ,  $U_{i_c+2}$  de l'autre.

démonstration

Supposons  $i+1 \leq i_c$ ; élevons les identités tirées des récurrences de l'algorithme de Jacobi-Perron

$$x_{i-1} = q_i x_i + x_{i+1} \text{ et } y_{i-1} = q_i y_i + y_{i+1}$$

au carré; on trouve

$$s_{i-1}^2 - s_{i+1}^2 = q_i^2 s_i^2 + 2q_i(x_i x_{i+1} + y_i y_{i+1})$$

que nous minorons, puisque  $\forall i \ x_i x_{i+1} < 0$  et  $|x_i|$  croissante par

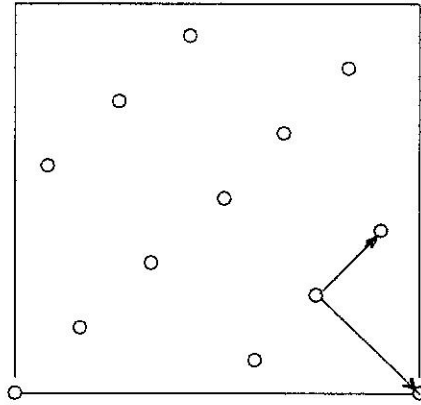
$$s_{i-1}^2 - s_{i+1}^2 \geq 2q_i(y_{i+1}^2 - x_{i+1}^2) \geq (y_{i_c}^2 - x_{i_c}^2) \geq 0$$

Par contre si  $i-1 \geq i+1$  on a

$$s_{i+1}^2 - s_{i-1}^2 \geq 2q_i(x_{i-1}^2 - y_{i-1}^2) \geq (x_{i+1}^2 - y_{i+1}^2) > 0$$

ce qui démontre l'assertion.

$$\frac{a}{b} = \frac{7}{12}$$



Les vecteurs minimaux; la base minimale.

fig. 1

Il est ensuite facile, en considérant les bases euclidiennes contenues dans les deux triangles précédents de déterminer les minima du réseau et une base minimale.

Nous verrons plus loin comment ces bases minimales interviennent dans quelques questions générales d'intersection.

### 3 Les continuants et les fins de paliers des droites discrètes

Les continuants donnent une autre façon d'exprimer les fins de paliers des droites discrètes. Nous venons de voir comment ils décrivent l'enveloppe convexe du réseau des restes dans le carré des périodes et nous connaissons la relation établie au §V entre ce convexe et les fins de paliers. Nous en déduisons une relation entre les fins de paliers et les continuants.

Soit  $\frac{a}{b}$  un rationnel dont le développement en fraction continue est  $[0; q_1, q_2, q_3, q_4, \dots, q_n, 1]$ , désignons par  $K_i$  la valeur du continuant  $K_i(q_1, \dots, q_i)$ ; alors nous avons le résultat suivant.

#### Théorème 1

L'ensemble des fins de paliers de la droite de pente  $\frac{a}{b}$  contenus dans la période  $[0, b-1]$  coïncide avec l'ensemble des combinaisons linéaires  $\alpha_1 K_1 + \alpha_2 K_2 + \dots + \alpha_{n-1} K_{n-1}$  où les coefficients entiers  $\alpha_i$  sont soumis aux

contraintes suivantes:

$$\alpha_1 \in [1, q_2], \alpha_2 \in [1, q_3], \dots, \alpha_{n-1} \in [1, q_n].$$

Nous pouvons tirer du théorème précédent un arbre de recouvrement minimal des points du réseau des restes à l'aide des vecteurs euclidiens. Il est également en relation avec la recherche des solutions d'inégalités diophantiennes.

## VII LE CLIVAGE D'UN RATIONNEL

Nous avons vu au IV prop. 9 que la longueur des paliers du mot de paliers d'un rationnel  $\frac{a}{b}$  est décrite par un rationnel; en introduisant le mot de paliers de ce dernier nous pouvons itérer ce processus; ceci conduit naturellement à une suite de rationnels associés à  $\frac{a}{b}$ , et à leurs mots de paliers. L'étude de cette suite de rationnels, voisine de la suite des réduites de  $\frac{a}{b}$ , fait l'objet de ce paragraphe; nous trouvons un résultat très général montrant comment la structure d'une droite discrète (par l'intermédiaire de son mot de palier) est reliée à celles d'autres droites discrètes. Le contenu géométrique sous-jacent se décrit comme suit. Alors qu'un segment euclidien, dès lors qu'il est subdivisé par quelques points est réunion des sous-segments induits il en va tout différemment en Géométrie Discrète: un segment n'est pas, sans précautions réunion de ses sous-segments. Les conditions sous lesquelles ceci est vrai sont décrites par le théorème suivant. Quelques cas très particuliers de ce résultat ont été abordés par les spécialistes de l'infographie; nous retrouvons bien sûr l'un d'eux, du à Wu [120], mais ici on va plus loin et la méthode est bien différente. De plus le "clivage" que nous introduisons plus loin permet de parcourir plus rapidement la suite des restes euclidiens du couple (a,b) en évitant un 1 sur 2 dans les séquences formées de 1 (un bénéfice de 50% pour les nombres de Fibonacci par exemple); nous donnons plusieurs algorithmes utilisant cet avantage.

### 1 Le théorème du mélange des mots de paliers

Soit  $[0; q_1, q_2, q_3, q_4, \dots]$  le développement en fraction continue du rationnel  $\frac{a}{b}$ . Son mot de paliers est long dominant si et seulement si  $q_2=1$  et court dominant si et seulement si  $q_2 > 1$ .

La transformation rationnelle  $\frac{a}{b} \longrightarrow \frac{a}{b+a-\{\frac{b}{a}\}}$ , dite de conjugaison,

échange les longs et courts dominants.

Théorème 1

Soit  $\frac{a}{b}$  le rationnel dont le développement en fraction continue est  $[0; q_1, q_2, q_3, q_4, \dots, q_p, q_{p+1}, \dots, q_n]$  et  $\frac{a}{b}$  celui dont le développement est  $[0; q_p, q_{p+1}, \dots, q_n]$ ; alors si  $\frac{a}{b}$  est long dominant (ie  $q_2=1$ ) son mot de paliers s'obtient en remplaçant dans la suite des restes  $\left\{ \frac{a \cdot i}{b} \right\}$  les termes  $\leq a_p$  par le mot de paliers de  $[0; q_1, q_2, q_3, q_4, \dots, q_{p-1}]$  et les termes  $> a_p$  par celui de  $[0; q_1, q_2, q_3, q_4, \dots, q_{p-1} + 1]$ .

Si  $\frac{a}{b}$  est court dominant (ie  $q_2 \geq 2$ ) son mot de palier s'obtient en remplaçant dans la suite des restes  $\left\{ \frac{a \cdot i}{b} \right\}$  retournée les termes  $< (b - a_p)$  par le mot de  $[0; q_1, q_2, q_3, q_4, \dots, q_{p-1}]$  et les termes  $\geq (b - a_p)$  par celui de  $[0; q_1, q_2, q_3, q_4, \dots, q_{p-1} + 1]$ .

Le rationnel  $\frac{a}{b}$  joue le rôle d'un mélangeur alors que la réduite  $[0; q_1, q_2, q_3, q_4, \dots, q_{p-1}]$  et sa perturbée  $[0; q_1, q_2, q_3, q_4, \dots, q_{p-1} + 1]$  se comportent comme des ingrédients.

La preuve de ce théorème nous conduit à étudier la suite des rationnels associés aux réduites de son développement en fraction continue du point de vue des mots de paliers.

2 Une suite de rationnels liée aux paliers des droites discrètes.

Dans ce paragraphe nous montrons que tout rationnel peut s'écrire comme action du produit de composition de fonctions homographiques particulières,  $\lambda(q)$  et  $\gamma(q)$ , dépendant d'un paramètre entier, sur des rationnels qui sont les inverses d'entiers. Cette structure est compatible avec la relation d'équivalence sur les rationnels induite par le mot de paliers: deux entiers sont "équivalents" si et seulement s'ils ont le même mot de paliers. C'est une différence avec le mot de Christoffel qui distingue tous les rationnels. De plus c'est cette structure qui est pertinente pour le dévissage du mot de paliers.

Soit  $\frac{a}{b} = [0; q_1, \dots, q_p]$  un rationnel  $\frac{a}{b}$  de l'intervalle  $[0,1]$ , développé en fraction continue. Nous introduisons la sous-suite  $v_i$  de la suite des indices des quotients partiels définie par

$$q_{v_i} > 1$$

et la notion suivante distinguant certains quotients partiels.

Définition 1

Nous dirons que le quotient partiel  $q_i$ , où  $i \in \{1, 2, \dots, p\}$ , est lié si et seulement si l'on a

$$\left\{ \begin{array}{l} q_i > 1 \\ \text{ou} \\ q_i = 1 \text{ et si } k \text{ vérifie } \nu_k < i < \nu_{k+1} \text{ alors } i - \nu_k \text{ pair} \\ \text{ou } i \text{ pair si } \nu_1 > 1 \text{ et } i < \nu_1. \end{array} \right.$$

Soit  $n$  le nombre de quotients partiels liés et  $\rho_i$  la suite des indices tels que  $q_{\rho_i}$  est lié,  $i=1, 2, \dots, n$  et où nous posons, par convention,  $\rho_0 = -1$ ; cette convention sera valable dans toute la suite. Par définition nous avons la

proposition 1

$q_1$  est toujours lié.

Les différences  $\rho_i - \rho_{i-1}$  sont égales à 1 ou 2; les quotients partiels liés sont soit consécutifs soit distants de deux unités.

Nous introduisons la suite des restes  $r_i$  de l'algorithme d'Euclide du couple  $(a, b)$ , définie par

$$r_{p+1} = 0, r_p = 1 \text{ et } r_{i-1} = q_i r_i + r_{i+1} \text{ où } i=p, \dots, 1.$$

Il est bien connu que  $r_0 = b$  et  $r_1 = a$ . Nous définissons maintenant une suite de rationnels  $\frac{a_i}{b_i}$ ,  $i=1, \dots, n$ , quotients des restes  $r_i$  pour les indices des quotients partiels liés; plus précisément:

$$\frac{a_i}{b_i} = \begin{cases} \frac{r_{\rho_i}}{r_{\rho_{i-1}}} & \text{si } \rho_i - \rho_{i-1} = 2 \\ \frac{r_{\rho_i}}{r_{\rho_{i-1}} - r_{\rho_i}} & \text{si } \rho_i - \rho_{i-1} = 1 \end{cases} \quad \text{où } i=1, \dots, n.$$

Les rationnels  $\frac{a_i}{b_i}$  s'expriment également à l'aide des quotients partiels  $q_i$  ou, ce qui revient au même, leurs développements en fractions continues sont liés à celui de  $\frac{a}{b}$ .

proposition 2

Nous avons  $\frac{a_i}{b_i} = [q_{\rho_i}, q_{\rho_i+1}, \dots, q_p]$  où  $q_{\rho_i} = \begin{cases} q_{\rho_i} & \text{si } \rho_i - \rho_{i-1} = 2 \\ q_{\rho_i}^{-1} & \text{si } \rho_i - \rho_{i-1} = 1 \end{cases}$

pour  $i=1, \dots, n$ .

On vérifie sans difficulté que l'on a les relations  $\frac{a_1}{b_1} = \frac{a}{b}$  et que  $\frac{a_n}{b_n} = \frac{1}{q_1}$  ou  $\frac{1}{q_1^{-1}}$ . Le résultat essentiel concernant la suite  $\frac{a_i}{b_i}$  est donné par la proposition suivante:

proposition 3

Soient  $\frac{a_{i+1}}{b_{i+1}}$  et  $\frac{a_i}{b_i}$  deux termes consécutifs de la suite de rationnels précédente alors on a les égalités suivantes:

$$a_{i+1} = \inf \left( \left\{ \frac{b_i}{a_i} \right\}, a_i - \left\{ \frac{b_i}{a_i} \right\} \right),$$

où  $\left\{ \frac{b_i}{a_i} \right\}$  représente le résidu de  $b_i$  modulo  $a_i$ , et

$$b_{i+1} = \sup \left( \left\{ \frac{b_i}{a_i} \right\}, a_i - \left\{ \frac{b_i}{a_i} \right\} \right).$$

Nous noterons l'application  $t\left(\frac{u}{v}\right) = \frac{\inf\left(\left\{\frac{v}{u}\right\}, u - \left\{\frac{v}{u}\right\}\right)}{\sup\left(\left\{\frac{v}{u}\right\}, u - \left\{\frac{v}{u}\right\}\right)}$ .

La démonstration de cette relation est immédiate. Il en résulte que la suite  $\frac{a_i}{b_i}$   $i=1, \dots, n$  se termine par un rationnel de la forme  $\frac{1}{m}$ . De plus nous pouvons exprimer assez simplement l'opération inverse permettant de passer de  $\frac{a_{i+1}}{b_{i+1}}$  à  $\frac{a_i}{b_i}$ .

proposition 4

Si le rationnel  $\frac{a}{b}$  est décomposé en fraction continue,  $\frac{a}{b} = [0; q_1, q_2, \dots]$ , nous avons la relation

$$\theta(q_1) \circ t\left(\frac{a}{b}\right) = \frac{a}{b} \quad \text{où } \theta = \begin{cases} \gamma & \text{si } q_2 \text{ est lié} \\ \lambda & \text{si } q_2 \text{ n'est pas lié.} \end{cases}$$

Autrement dit nous pouvons inverser l'application  $t$ . Si nous posons  $t(\frac{a}{b}) = \frac{a'}{b'}$ , alors  $q_2$  est lié si et seulement si nous avons  $2a' > b'$ . Ceci nous permet également de déterminer la réciproque de  $t$  sans faire appel aux quotients partiels.

corollaire 1

Pour deux rationnels consécutifs de la suite  $\frac{a_i}{b_i}$  comme ci-dessus nous avons l'égalité

$$\frac{a_i}{b_i} = \begin{cases} \frac{a_{i+1} + b_{i+1}}{\tilde{q}_i(a_{i+1} + b_{i+1}) + a_{i+1}} & \text{si } \rho_{i+1} - \rho_i = 1 \\ \frac{a_{i+1} + b_{i+1}}{\tilde{q}_i(a_{i+1} + b_{i+1}) + b_{i+1}} & \text{si } \rho_{i+1} - \rho_i = 2 \end{cases}$$

$$\text{où } \tilde{q}_i = \begin{cases} q_{\rho_{n+1-i}} & \text{si } \rho_{n+1-i} - \rho_{n-1} = 2 \\ q_{\rho_{n+1-i}} - 1 & \text{si } \rho_{n+1-i} - \rho_{n-1} = 1. \end{cases}$$

Nous appellerons quotients partiels corrigés les  $\tilde{q}_i$ ; ils sont égaux aux quotients partiels liés ou aux quotients partiels liés diminués de 1.

Remarques:

Comme  $q_1$  est toujours lié et d'après notre convention  $\rho_0 = -1$  on a toujours  $\tilde{q}_{\rho_1} = q_{\rho_1} = q_1$ .

Toutes les notions de quotients liés, quotients corrigés etc... sont compatibles avec la relation d'équivalence induite sur les fractions continues par l'égalité  $[0; q_1, q_2, \dots, q_p, 1] = [0; q_1, q_2, \dots, q_p + 1]$ .

La suite de fractions  $\frac{a_i}{b_i}$  peut être reconstituée à partir de  $\frac{a_n}{b_n}$  jusqu'à  $\frac{a_1}{b_1} = \frac{a}{b}$  par le procédé suivant.

Si  $\frac{u}{v}$  est un rationnel  $< 1$  et  $e$  un entier nous posons

$$\lambda(e)(\frac{u}{v}) = \frac{u+v}{e(u+v)+v}$$

et

$$\gamma(e)\left(\frac{u}{v}\right) = \frac{u+v}{e(u+v)+u}.$$

Il est clair que notre suite de rationnels est donné par la suite de composition suivante:

$$\frac{a_n}{b_n} \xrightarrow{\theta(e_{n-1})} \frac{a_{n-1}}{b_{n-1}} \xrightarrow{\theta(e_{n-2})} \frac{a_{n-2}}{b_{n-2}} \dots \xrightarrow{\theta(e_1)} \frac{a_1}{b_1} = \frac{a}{b}$$

$$\text{où } \theta(e_{i-1}): \frac{a_i}{b_i} \longrightarrow \frac{a_{i-1}}{b_{i-1}} = \begin{cases} \lambda(e_{i-1}) & \text{si } \rho_i - \rho_{i-1} = 2 \\ \gamma(e_{i-1}) & \text{si } \rho_i - \rho_{i-1} = 1 \end{cases}$$

autrement dit nous avons

$$\frac{a}{b} = \theta(e_1) \circ \theta(e_2) \circ \dots \circ \theta(e_{n-1}) \left( \frac{a_n}{b_n} \right)$$

où  $\frac{a_n}{b_n}$  est l'inverse d'un entier. C'est le clivage du rationnel  $\frac{a}{b}$ .

Plus précisément nous avons l'énoncé suivant

#### corollaire 2

Soit  $\frac{a}{b} = [q_1, q_2, \dots, q_p]$  le développement en fraction continue du rationnel  $\frac{a}{b}$ , et  $\rho_i$ ,  $i=1, \dots, n$  la suite des indices des quotients partiels liés et  $\tilde{q}_{\rho_i}$  les quotients partiels corrigés:

$$\tilde{q}_{\rho_i} = \begin{cases} q_{\rho_i} & \text{si } \rho_i - \rho_{i-1} = 2 \\ q_{\rho_i} - 1 & \text{si } \rho_i - \rho_{i-1} = 1 \end{cases}$$

alors le clivage de  $\frac{a}{b}$  est donné par

$$\frac{a}{b} = \theta(\tilde{q}_{\rho_1}) \circ \theta(\tilde{q}_{\rho_2}) \circ \dots \circ \theta(\tilde{q}_{\rho_{n-1}}) \left( \frac{1}{\tilde{q}_{\rho_n}} \right)$$

L'intérêt de cette notion résulte dans le fait qu'elle contrôle très exactement le mot de paliers de  $\frac{a}{b}$  comme nous le verrons dans la dernière partie.

D'après nos définitions nous avons également un procédé très simple de détermination du type de l'opérateur  $\lambda$  ou  $\gamma$  qui intervient à chaque étape du clivage; si nous posons  $t\left(\frac{a}{b}\right) = \frac{a'}{b'}$ , alors  $\frac{a}{b} = \gamma(e)\left(\frac{a'}{b'}\right)$  si  $a' = \left\langle \frac{b}{a} \right\rangle$  et  $\frac{a}{b} = \lambda(e)\left(\frac{a'}{b'}\right)$  si  $b' = \left\langle \frac{b}{a} \right\rangle$  où  $e = \left[ \frac{b}{a} \right]$ .

Remarquons que le nombre d'opérateurs  $\Theta$  intervenant dans le clivage est généralement plus court que le nombre d'étapes de l'algorithme d'Euclide (ou nombre de quotients partiels du développement en fraction continue) puisque nous retirons environ un terme sur deux dans les séquences de 1 de la suite des quotients partiels.

exemple

Soit  $\alpha = \frac{16}{33} = [0; 2, 16]$ , alors  $q_1=2$  et  $q_2=16$  sont liés, la suite des  $\tilde{q}_{p_i}$  est 2, 15 et son clivage:

$$\frac{16}{33} = \gamma(2)\left(\frac{1}{15}\right).$$

### 3 Le dévissage et la reconstruction d'un mot de paliers.

Le mot de paliers est un élément de l'ensemble  $\mathcal{M}$  formé par les mots sur deux lettres  $l$  et  $c$  dont l'une est isolée et dont les paliers formés par l'autre ont des longueurs consécutives.

Le clivage d'un rationnel  $\frac{a}{b}$  correspond à une décomposition du mot de paliers de  $\frac{a}{b}$  de la façon suivante: aux opérateurs  $\lambda, \gamma, t$  agissant sur  $\mathbb{Q}$  correspondent des morphismes  $\Lambda, \Gamma$  et  $T$  de  $\mathcal{M}$  qui rendent les diagrammes suivants commutatifs:

$$\begin{array}{ccc} \mathbb{Q} \xrightarrow{\mu} \mathcal{M} & \mathbb{Q} \xrightarrow{\mu} \mathcal{M} & \mathbb{Q} \xrightarrow{\mu} \mathcal{M} \\ t \downarrow & \lambda \downarrow & \gamma \downarrow \\ \mathbb{Q} \xrightarrow{\mu} \mathcal{M} & \mathbb{Q} \xrightarrow{\mu} \mathcal{M} & \mathbb{Q} \xrightarrow{\mu} \mathcal{M} \\ & \downarrow T & \downarrow \Lambda \\ & \mathbb{Q} \xrightarrow{\mu} \mathcal{M} & \downarrow \Gamma \\ & & \mathbb{Q} \xrightarrow{\mu} \mathcal{M} \end{array}$$

L'opérateur  $T$  agit sur un mot en associant  $l$  aux paliers longs formés par la lettre dominante et un  $c$  aux paliers courts.

Les opérateurs  $\Lambda$  forment une famille à un paramètre entier, ils sont définis d'abord sur les mots  $l$  et  $c$ :

$$\begin{cases} \Lambda(q)(l) = \underbrace{l \dots l}_{q+1} c \\ \Lambda(q)(c) = \underbrace{l \dots l}_q c \end{cases} \quad (1)$$

puis sur un mot  $m = m_1 \dots m_k$  nous posons  $\Lambda(q)(m) = \Lambda(q)(m_1) \dots \Lambda(q)(m_k)$

De même nous définissons les opérateurs  $\Gamma$ :

$$\begin{cases} \Gamma(q)(\ell) = \underbrace{lc\dots c}_{q+1} \\ \Gamma(q)(c) = \underbrace{lc\dots c}_q \end{cases} \quad (1')$$

puis sur  $m$  nous posons  $\Gamma(q)(m) = \Gamma(q)(m_k)\dots\Gamma(q)(m_1)$ , ie nous retournons le mot.

La commutativité des diagrammes se montre sans difficulté. De plus nous avons la relation suivante.

proposition 5

Soit  $m = \mu(\frac{a}{b})$  le mot de paliers du rationnel  $\frac{a}{b} = [0; q_1, q_2, \dots]$  alors on a

$$\Theta(q_2) \circ T(m) = m \text{ où } \Theta = \begin{cases} \Gamma \text{ si } q_2 \text{ est lié} \\ \Lambda \text{ si } q_2 \text{ n'est pas lié.} \end{cases}$$

Le premier quotient partiel n'intervient pas dans le mot de paliers  $m$ .

Ceci montre par "fonctorialité" que  $\mu(\frac{a}{b})$  se décompose et se reconstruit simplement grace au clivage de  $\frac{a}{b}$ . Nous aboutissons au théorème de structure

Théorème 1

Soit  $\frac{a}{b} = [q_1, q_2, \dots, q_p]$  le développement en fraction continue du rationnel  $\frac{a}{b}$ , et  $\rho_i, i=1, \dots, n$  la suite des indices des quotients partiels liés et  $\tilde{q}_{\rho_i}$  les quotients partiels corrigés:

$$\tilde{q}_{\rho_i} = \begin{cases} q_{\rho_i} & \text{si } \rho_i - \rho_{i-1} = 2 \\ q_{\rho_i} - 1 & \text{si } \rho_i - \rho_{i-1} = 1 \end{cases}$$

de sorte que le clivage de  $\frac{a}{b}$  est donné par

$$\frac{a}{b} = \Theta(\tilde{q}_{\rho_1}) \circ \Theta(\tilde{q}_{\rho_2}) \circ \dots \circ \Theta(\tilde{q}_{\rho_{n-1}}) \left( \frac{1}{\tilde{q}_{\rho_n}} \right)$$

alors

$$\mu(\frac{a}{b}) = \Theta(\tilde{q}_{\rho_2}) \circ \Theta(\tilde{q}_{\rho_3}) \circ \dots \circ \Theta(\tilde{q}_{\rho_n})(c)$$

Le théorème du mélange s'en déduit sans difficulté.

exemples

1° Prenons  $\frac{a}{b} = \frac{7}{24} = [0; 3, 2, 3]$ , ses quotients partiels réduits sont 3, 1, 2; son clivage est:

$$\frac{7}{24} \xleftarrow{\gamma(3)} \frac{3}{4} \xleftarrow{\gamma(1)} \frac{1}{2},$$

la décomposition du mot  $\mu(\frac{7}{24})$  est donc:

$$\mu(\frac{7}{24}) \xleftarrow{\Gamma(1)} \mu(\frac{3}{4}) \xleftarrow{\Gamma(2)} \mu(\frac{1}{2}) = c,$$

ce qui donne  $\mu(\frac{3}{4}) = lcc$  et  $\mu(\frac{7}{24}) = lclclcc$ .

2° Soit  $\frac{a}{b} = \frac{16}{25} = [1, 1, 1, 3, 1, 1]$ , dont le clivage est

$$\frac{16}{25} \xleftarrow{\lambda(1)} \frac{7}{9} \xleftarrow{\gamma(1)} \frac{2}{5} \xleftarrow{\lambda(2)} \frac{1}{1}$$

soulignons les  $q_i$  liés:

$$\frac{a}{b} = [1, 1, 1, \underline{3}, 1, 1]$$

les quotients partiels réduits valent 1, 1, 2, 1, la décomposition de  $\mu(\frac{a}{b})$  est donnée par:

$$\Lambda(1) \circ \Gamma(2) \circ \Lambda(1)(c)$$

soit  $\mu(\frac{a}{b}) = llclclclclclclclc$ .

Le rationnel  $\frac{a}{b}$  vaut  $\frac{16}{25}$ , sa suite des restes  $\left\{ \frac{a_i}{b} \right\}$  associée vaut

$$\underline{0} \quad \underline{16} \quad \underline{7} \quad \underline{23} \quad \underline{14} \quad \underline{5} \quad \underline{21} \quad \underline{12} \quad \underline{3} \quad \underline{19} \quad \underline{10} \quad \underline{1} \quad \underline{17} \quad \underline{8} \quad \underline{24} \quad \underline{15} \quad \underline{6} \quad \underline{22} \quad \underline{13} \quad \underline{4} \quad \underline{20} \quad \underline{11} \quad \underline{2} \quad \underline{18} \quad \underline{9}$$

où nous avons distingué les paliers; nous retrouvons bien le mot de paliers précédent.

3° Le rationnel  $\frac{41}{69}$  s'écrit  $\Lambda(1)\Gamma(2)\Lambda(5)\Gamma(1)(\frac{0}{1})$ ; plus précisément nous avons le clivage:

$$\frac{0}{1} \xrightarrow{\Gamma(1)} \frac{1}{1} \xrightarrow{\Lambda(5)} \frac{2}{11} \xrightarrow{\Gamma(2)} \frac{13}{28} \xrightarrow{\Lambda(1)} \frac{41}{69}.$$

Si nous voulons déterminer le mot de paliers de  $\frac{41}{69}$  nous partons de la décomposition canonique précédente et formons le produit d'opérateurs:

$\Lambda(2)\Gamma(5)\Lambda(1)(c)$ ; ceci donne successivement

$$lc,$$

$$lccccclcccccc,$$

et

lllclllclllclllclllclllclllclllclllclllc,

qui est bien le mot de paliers de  $\frac{41}{69}$ .

4° Terminons avec  $\frac{a}{b} = \frac{8529}{13312} = [1,1,1,3,1,1,1,1,2,1,1,1,3,1,1,1,1]$ , soulignons les  $q_i$  liés:

$$\frac{a}{b} = [1,1,1,3,1,1,1,1,2,1,1,1,3,1,1,1,1]$$

Nous laissons au lecteur le soin de déterminer le clivage de ce rationnel; la décomposition du mot de paliers est donnée par le produit de composition suivant:

$$\Lambda(1) \circ \Gamma(2) \circ \Lambda(1) \circ \Lambda(1) \circ \Gamma(1) \circ \Lambda(1) \circ \Lambda(2) \circ \Lambda(1) \circ \Lambda(1)(c)$$

#### 4 Algorithmes de construction d'un mot de paliers; nouveaux tracés.

Nous aboutissons finalement à un autre type d'algorithmes de tracé d'une droite naïve via son mot de paliers; d'après le théorème de structure tout revient d'abord à déterminer le clivage du rationnel puis à calculer un produit de composition d'homomorphismes de la forme

$$\Theta(n_1) \circ \Theta(n_2) \circ \dots \circ \Theta(n_p)(c) \quad (1)$$

où  $\Theta$  est comme ci-dessus. Nous pouvons évaluer cette expression de deux façons.

Le premier algorithme qui s'impose utilise les règles de remplacement précédentes, c'est une évaluation de droite à gauche de (1). Mais lors d'une évaluation de la forme  $\Gamma(n)(m)$  où  $m$  est un mot sur les lettres  $l$  et  $c$  il est nécessaire de retourner  $m$ ; ceci n'est pas une opération simple réalisable par un automate fini. Bien qu'une implémentation machine soit possible nous allons donner un autre algorithme pour lequel le retournement n'est plus imposé sous cette forme stricte. Ce nouvel algorithme est implémentable sur un automate à pile.

La détermination de (1) peut être conduite de gauche à droite à condition d'évaluer simultanément les deux suites  $\Theta(n_1) \circ \dots \circ \Theta(n_k)(l)$  et  $\Theta(n_1) \circ \dots \circ \Theta(n_k)(c)$  pour  $k=1,2,3,\dots$ . Si nous désignons par  $m_{k-1}$  et  $m'_{k-1}$  ces deux mots  $m_{k-1} = \Theta(n_1) \circ \dots \circ \Theta(n_{k-1})(l)$  et  $m'_{k-1} = \Theta(n_1) \circ \dots \circ \Theta(n_{k-1})(c)$  lorsque l'indice vaut  $k-1$  alors nous pouvons former  $m_k = \Theta(n_1) \circ \dots \circ \Theta(n_k)(l)$ , (resp  $m'_k = \Theta(n_1) \circ \dots \circ \Theta(n_k)(c)$ ) en remplaçant les  $l$  en  $m$  et les  $c$  en  $m'$  dans le mot  $\Theta(n_k)(l)$  (resp  $\Theta(n_k)(c)$ ) selon les relations (1) et (1') du § précédent.

D'où l'algorithme suivant dans lequel  $\prod_{k-1}$  désigne le produit









le lecteur pourra constater la coïncidence de cette structure avec celle que donne l'algorithme:

$$\mu\left(\frac{51}{91}\right) = \text{llllcllllcllllcllllcllllcllllcllllcllllcllllc}$$

### 5 Les droites naïves et les mots de Sturm.

Dans cette dernière partie nous établissons un lien entre les droites naïves et les mots de Sturm nous permettant de les dénombrer. Notre préoccupation, ici, n'est plus algorithmique mais didactique, car nous pensons que l'approche la plus arithmétique possible peut clarifier certains résultats. La méthode introduite ici ressemble beaucoup à celle du clivage mais diffère dans le détail.

Nous utilisons ici la notion de code d'une droite naïve de pente rationnelle  $\frac{a}{b}$  où  $0 \leq a < b$ , à savoir sa dérivée discrète

$$\text{cd}\left(\frac{a}{b}\right)(i) = \left[ \frac{a(i+1)}{b} \right] - \left[ \frac{ai}{b} \right]$$

qui est une suite illimitée dans les deux sens de 0 et de 1 valant 0 sur les paliers de la droite sauf aux fins de paliers où elle vaut 1.

Par exemple si  $\frac{a}{b} = \frac{5}{17}$  son code vaut

$$\text{cd}\left(\frac{5}{17}\right)(i) = \dots 00010010001001001\dots$$

Cette égalité donne les valeurs du code pour  $i \in [0, 16]$ ; pour des  $i$  différents il s'obtient par périodicité. Il est commode, comme dans d'autres domaines, de désigner alors le code du rationnel  $\frac{a}{b}$  par le symbole

$$\text{cd}\left(\frac{a}{b}\right) = (0\dots 1)^\infty$$

où le contenu de la parenthèse désigne la valeur du code sur une période.

#### Mots de Sturm.

D'après Morse et Hedlung un mot de sturm  $\mathcal{S}$  sur deux symboles 0 et 1 est une suite illimitée  $\mathcal{S} = (x_i)_{i \in \mathbb{Z}}$ ,  $x_i \in \{0, 1\}$ , vérifiant les conditions suivantes:

$$\forall a, b, c, d \in \mathbb{Z} \text{ tels que } |a-b| = |c-d| \text{ alors } \left| \sum_{a \leq i \leq b} x_i - \sum_{c \leq i \leq d} x_i \right| \leq 1$$

Nous nous intéressons dans la suite aux mots de Sturm périodiques, ie où  $\mathcal{S} = (s)^\infty$   $s$  étant un mot sur l'alphabet  $\{0, 1\}$ , ainsi qu'aux mots de Sturm primitifs, c'est à dire ceux pour lesquels la décomposition précédente est "minimale".

Nous ne distinguons pas les mots de Sturm qui se déduisent les uns des autres par translation. Ainsi, pour nous, les mots de Sturm  $(001)^\infty$  et  $(010)^\infty$

sont égaux. Un mot de Sturm primitif de longueur  $n$  ainsi défini correspondra à  $n$  symboles  $s$  différents obtenus par permutations circulaires et donnant le même mot infini  $\mathcal{P} = (s)^\infty$ .

### Propriétés des mots de Sturm.

#### 1 Allongement régulier d'un mot de Sturm

Si  $m = \{x_i\}_{i \in \mathbb{Z}}$  est un mot de  $\{0,1\}^*$  et  $k$  un entier positif ou nul nous désignons par  $al(k)$  l'opérateur défini de la manière suivante:

si  $k \geq 1$  et si  $\{i | x_i = 1\} \neq \emptyset$   $al(k)(m)$  est obtenu en remplaçant chaque 1 par  $0^k 1$

si  $k=0$  ou si  $\{i | x_i = 1\} = \emptyset$  alors  $al(k)(m) = m$ .

Il est clair que si  $\mathcal{P}$  est Sturm alors  $al(k)(\mathcal{P})$  est Sturm.

#### 2 Conjugué d'un mot de Sturm

Si  $m = \{x_i\}_{i \in \mathbb{Z}}$  est un mot de  $\{0,1\}^*$  nous désignons par  $\sigma(m)$  le mot obtenu en échangeant les 0 et 1 et en retournant  $m$ ; plus précisément

$$\sigma(m) = \{\bar{x}_{-i}\}_{i \in \mathbb{Z}} \text{ où } \bar{0} = 1 \text{ et } \bar{1} = 0.$$

Nous avons également la propriété évidente suivante:

Si  $\mathcal{P}$  est Sturm  $\sigma(\mathcal{P})$  est Sturm.

3 Le code d'un rationnel est Sturm; ceci résulte des propriétés des séquences montantes des droites naïves.

#### 4 Compatibilité entre les codes naïfs et les mots de Sturm.

Les résultats suivants résultent également des propriétés des séquences montantes: si  $\mathcal{P}$  est le code de  $\frac{a}{b}$  alors  $al(k)(\mathcal{P})$  est le code de  $\frac{a}{b + ka}$  et  $\sigma(\mathcal{P})$  est le code de  $\frac{b-a}{b}$ , (nous rappelons que  $0 \leq a < b$ ).

Ces deux dernières propriétés vont nous permettre de montrer que tout mot de Sturm est le code d'un rationnel.

#### Mots de Sturm et algorithme d'Euclide

Les propriétés suivantes des mots de Sturm se démontrent facilement.

-Si  $\mathcal{P}$  est Sturm les 0 ou les 1 sont isolés et la lettre non isolée forme des paliers dont les longueurs sont deux entiers consécutifs  $k$  et  $k+1$ .

-Soit  $\mathcal{P}$  un mot de Sturm dont les 1 sont isolés et dont les paliers de 0 sont de longueur  $k$  ou  $k+1$  nous désignons par  $cp(k)(\mathcal{P})$  le mot de Sturm "comprimé" obtenu en remplaçant les sous-mots  $0^k 1$  par 1 et les sous-mots  $0^{k+1} 1$  par  $01$ . Ce mot est bien de Sturm et cette fois les 0 sont isolés. Il est facile de

vérifier que  $cp(k)$  est l'inverse de  $al(k)$ .

-Si  $\mathcal{S}$  est un mot de Sturm l'opérateur  $\sigma$  échange le rôle des lettres isolées.

Le lien entre les deux objets sera établi en remarquant que l'application des opérateurs  $cp(k)$  et  $\sigma$  à un mot de Sturm  $\mathcal{S}$  aboutit toujours au mot  $(1)^\infty$ ; c'est une variante de l'algorithme d'Euclide interprété sur les mots de Sturm. Comme les opérateurs  $cp(k)$  et  $\sigma$  sont des automorphismes le mot  $\mathcal{S}$  peut être reconstruit à partir du mot  $(1)^\infty$  (ou de  $(0)^\infty$ ) et s'écrit sous la forme suivante:

$$\mathcal{S} = al(k_1) \circ \sigma \circ al(k_2) \circ \sigma \circ \dots \circ al(k_n) (1)^\infty$$

D'après la propriété 4 de compatibilité entre les codes naïfs et les mots de Sturm,  $\mathcal{S}$  est le code du rationnel dont le développement en fraction continue est  $[0; k_1+1, k_2, \dots, k_n]$ .

Finalement nous avons obtenu le résultat suivant:

#### Théorème 1

*Il existe une correspondance bijective entre les mots de Sturm périodiques et les rationnels de l'intervalle  $[0,1]$ . De plus, dans cette transformation les mots de Sturm primitifs de longueur  $b$  correspondent aux rationnels  $\frac{a}{b}$  vérifiant  $0 \leq a < b$  et  $(a,b)=1$ ; il existe donc  $\phi(b)$  mots de Sturm primitifs de longueur  $b$ ,  $\phi$  désignant la fonction d'Euler.*

Dans leurs fondement de la Dynamique Symbolique Morse et Hedlund [71] ont introduit indépendamment diverses notions de mots dont certains dits "sturmiens" peuvent être rapprochés des mots de Christoffel. L'étude de ces mots a donné lieu à de nombreux travaux: Coven-Hedlung [27] et Rauzy [91] en particulier. Grace au développement en fraction continue nous établissons un lien entre les mots de Sturm et la dérivée discrète des droites naïves ce qui nous permet de retrouver très facilement la formule de dénombrement conjecturée par Dulucq et Gouyou-Beauchamp [38] et démontrée par Mignosi.

VIII EVALUATION D'UNE INTEGRALE DISCRETE ET APPLICATION AU DENOMBREMENT DE POINTS DE RESEAUX ET AU "LATTICE PROBLEM".

Les premiers éléments de géométrie discrète élaborés dans les paragraphes précédents font apparaître des "transcodages" arithmético-géométriques intéressants et qui, provoquant des rencontres entre des questions à priori éloignées comme les pixels et les minima de réseaux par exemple, font apparaître des réponses imprévues. Nous donnons ici un exemple utilisant le transcodage "nombre rationnel"- "droite discrète" pour transporter un peu de l'arithmétique d'un couple d'entier (i.e. l'algorithme d'Euclide) dans des problèmes de dénombrement de points entiers ou de points de réseaux très souvent étudiés (cf [18], [24], [30], [40], [41], [54], [112]). Nous trouvons en particulier une formule de dénombrement qui généralise celle de Pick (cf [84]) et donne une évaluation exacte du nombre de points entiers d'un triangle à sommets rationnels, le "lattice problem" qui remonte à Césaro (cf. [18]), Ramanujan et Hardy (cf [54]). Notons aussi au passage que notre évaluation de l'intégrale discrète généralise une sommation, (donnée par (1) ci-dessous), également étudiée à maintes reprises (cf Knuth [66], [47], Dieter [31]) elle même liée aux sommes de Dedekind (cf Rademacher et Grosswald [88]).

Ce calcul, intéressant pour la Géométrie de Nombres, nous permet de donner le nombre de points d'un réseau entier dans une fenêtre rectangulaire isothétique. Il pourrait être le point de départ d'une étude des divers "paramétrages" de droites discrètes d'épaisseurs quelconques. Nous n'avons pas entrepris ce travail. La complexité des formules obtenues montre, à notre avis, de façon très nette qu'il est beaucoup plus difficile de cheminer à travers la Géométrie de Nombres par voie purement analytique ou algébrique que par celle de la représentation géométrique ou graphique. Les droites discrètes sont des objets relativement simples dont les descriptions formelles sont beaucoup plus compliquées; il est heureux qu'elles possèdent une algorithmique conforme à leur géométrie et non à leur algèbre.

1 Le calcul d'une intégrale associée à une droite discrète.

Soit  $\frac{a}{b}$  un rationnel, nous voudrions évaluer l'intégrale discrète

$$I(b,a,x+1,y) = \sum_{i=x+1}^y \left[ \frac{ai}{b} \right] \quad (1)$$

qui représente le nombre de points entiers situés sous la droite discrète de pente  $\frac{a}{b}$  passant par l'origine entre les points d'abscisse  $x+1$  et  $y$ . Sur la figure 1 ci-dessous ces points entiers sont représentés par de petits carrés.

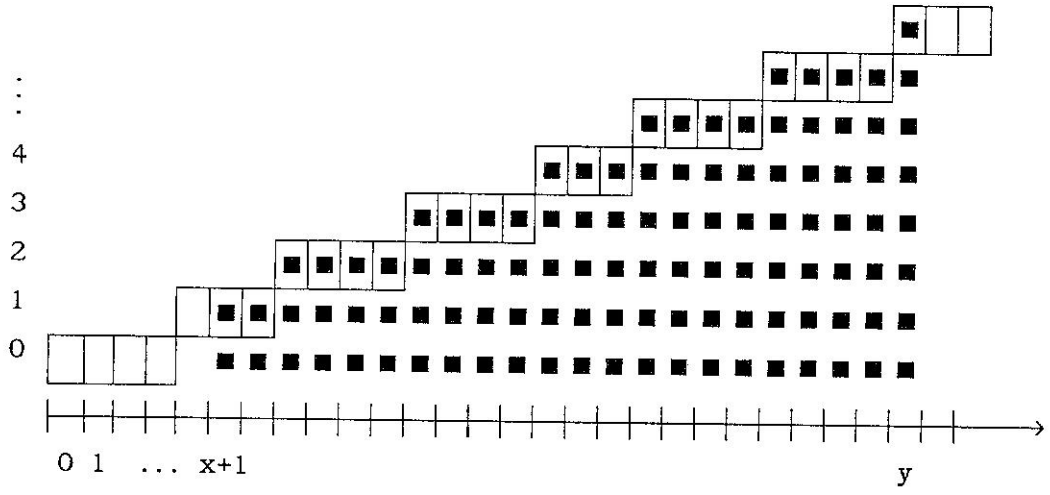


fig. 1

Une telle évaluation apparait dans le "lattice problem" de Ramanujan présenté par Hardy dans [54]; Césaro avait également étudié une question de ce type (cf. [18]); Knuth (cf [47] et [66]) a également étudié cette sommation. Alors que Césaro, Hardy et Ramanujan utilisent la sommation évidente par colonnes et cherchent ensuite un développement asymptotique de la somme nous allons suivre un chemin différent qui exploite la structure des paliers de la droite discrète.

Rappelons que la droite discrète (naïve) de pente rationnelle  $\frac{a}{b}$  passant par l'origine, (nous supposons aussi que  $0 < a < b \leq 1$  et que  $a$  et  $b$  sont premiers entre eux), est définie par l'ensemble des points  $(i, \left[\frac{ai}{b}\right])$  de  $\mathbb{Z}^2$  obtenu lorsque  $i$  parcourt  $\mathbb{Z}$ . Ce sous-ensemble de  $\mathbb{Z}^2$  est une réunion de "paliers" horizontaux formés par les points de même ordonnée. Si nous associons l'indice 1 au palier contenant l'origine puis les valeurs entières évidentes aux autres nous pouvons vérifier (cf IV prop. 1) que l'abscisse de la fin du  $k$ -ième palier est  $\left[\frac{kb-1}{a}\right]$ . Par exemple les abscisses des fins de paliers d'indices  $-2, -1, 0, 1, 2, 3$  de la droite discrète de pente  $\frac{5}{17}$  sont  $-7, -4, -1, 3, 6$  et  $10$ .

Nous désignons par  $\left[\frac{m}{n}\right]$  (resp.  $\left\{\frac{m}{n}\right\}$ ) le quotient (resp. le reste) de la division entière de  $m$  par  $n$ .

L'abscisse de la fin du palier qui précède  $x$  étant égale à  $\left[\frac{\left[\frac{ax}{b}\right]b-1}{a}\right]$ ,  
comme sur la figure suivante,

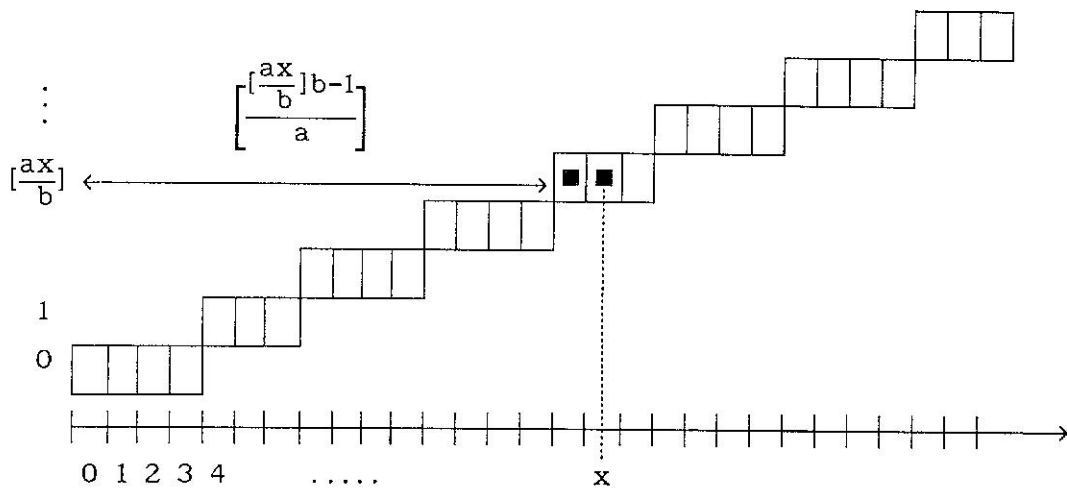


fig. 2

l'intégrale  $I(b,a,1,x)$  est égale à la somme des différences

$$\left(x - \left[ \frac{b-1}{a} \right]\right) + \left(x - \left[ \frac{2b-1}{a} \right]\right) + \left(x - \left[ \frac{3b-1}{a} \right]\right) + \dots + \left(x - \left[ \frac{[\frac{ax}{b}]b-1}{a} \right]\right)$$

soit, en regroupant,

$$I(b,a,1,x) = \left[ \frac{ax}{b} \right] x - \sum_{i=1}^{\left[ \frac{ax}{b} \right]} \left[ \frac{bi-1}{a} \right]$$

Extrayons les parties entières de la somme en utilisant les transformations

$$\left[ \frac{bi-1}{a} \right] = \frac{bi-1 - \left\{ \frac{bi-1}{a} \right\}}{a} = \frac{bi-1 - \left\{ \frac{b}{a} \right\} i-1}{a}$$

ce qui donne pour la dernière somme la relation

$$\sum_{i=1}^{\left[ \frac{ax}{b} \right]} \left[ \frac{bi-1}{a} \right] = \sum_{i=1}^{\left[ \frac{ax}{b} \right]} \frac{bi-1}{a} - \frac{1}{a} \sum_{i=1}^{\left[ \frac{ax}{b} \right]} \left\{ \frac{b}{a} \right\} i-1$$

et finalement

$$\sum_{i=1}^{\left[ \frac{ax}{b} \right]} \left[ \frac{bi-1}{a} \right] = \frac{b}{2a} \left[ \frac{ax}{b} \right] \left( \left[ \frac{ax}{b} \right] + 1 \right) - \frac{1}{a} \left[ \frac{ax}{b} \right] - \frac{1}{a} \sum_{i=1}^{\left[ \frac{ax}{b} \right]} \left\{ \frac{b}{a} \right\} i-1$$

En introduisant la fonction

$$\psi_1(b,a,x) = \frac{1}{2a} (2ax-b+2) \left[ \frac{ax}{b} \right] - \frac{b}{2a} \left[ \frac{ax}{b} \right]^2$$

l'intégrale cherchée s'écrit

$$I(b, a, x+1, y) = \psi_1(b, a, y) - \psi_1(b, a, x) + \frac{1}{a} \sum_{i=\left[\frac{ax}{b}\right]+1}^{\left[\frac{ay}{b}\right]} \left\{ \frac{\left(\frac{b}{a}\right)^{i-1}}{a} \right\}$$

La périodicité de la suite des restes  $\left\{ \frac{\left(\frac{b}{a}\right)^{i-1}}{a} \right\}$  et l'égalité:  $(\alpha+1)\left\{\frac{b}{a}\right\} = \left\{\frac{b}{a}\right\}-1$  vérifiée par  $\alpha = -\left\{\frac{b}{a}\right\}^{-1} \bmod a$  conduisent au lemme suivant:

lemme 1

*Pour tout couple d'entiers u et v nous avons l'égalité*

$$\sum_{i=u}^v \left\{ \frac{\left(\frac{b}{a}\right)^{i-1}}{a} \right\} = \sum_{i=u+\alpha}^{v+\alpha} \left\{ \frac{\left(\frac{b}{a}\right)^i}{a} \right\}$$

Appliquons le dans la dernière somme, il vient

$$I(b, a, x+1, y) = \psi_1(b, a, y) - \psi_1(b, a, x) + \frac{1}{a} \sum_{i=\left[\frac{ax}{b}\right]+\alpha+1}^{\left[\frac{ay}{b}\right]+\alpha} \left\{ \frac{\left(\frac{b}{a}\right)^i}{a} \right\}$$

Modifions à nouveau la somme ci-dessus en utilisant l'égalité

$$\left\{ \frac{\left(\frac{b}{a}\right)^i}{a} \right\} = \left\{ \frac{b}{a} \right\}^i - a \left[ \frac{\left(\frac{b}{a}\right)^i}{a} \right]$$

afin de revenir à une expression analogue à notre intégrale discrète initiale; tenons compte au passage de la modification de  $\psi_1$  provenant du terme  $\left\{\frac{b}{a}\right\}^i$  pour introduire la primitive discrète partielle d'une droite discrète, la fonction rationnelle:

$$\psi(b, a, x) = \frac{1}{2a} (2ax - b + 2 + (2\alpha+1)\left\{\frac{b}{a}\right\}) \left[ \frac{ax}{b} \right] + \frac{1}{2a} (\left\{\frac{b}{a}\right\} - b) \left[ \frac{ax}{b} \right]^2$$

Nous obtenons finalement l'identité

$$I(b, a, x+1, y) = \psi(b, a, y) - \psi(b, a, x) - I\left(a, \left\{\frac{b}{a}\right\}, x^* + 1, y^*\right) \quad (2)$$

où  $x^* = \alpha + \left[ \frac{ax}{b} \right]$  et  $y^* = \alpha + \left[ \frac{ay}{b} \right]$   $\alpha$  étant défini plus haut.

Cette dernière relation fait apparaître l'algorithme d'Euclide dans le calcul

de l'intégrale discrète. Changeons donc un peu nos notations, remplaçant  $b$  par  $a_0$ ,  $a$  par  $a_1$  et introduisons les suites définies pour  $i \geq 1$  comme ci-dessous:

$$a_{i+1} = \frac{a_{i-1}}{a_i}$$

$$\alpha_i = -a_{i-1}^{-1} \text{ mod } a_i \text{ pour } i \geq 1$$

$$x_i = \alpha_i + \left[ \frac{a_i x_{i-1}}{a_{i-1}} \right] \text{ et } y_i = \alpha_i + \left[ \frac{a_i y_{i-1}}{a_{i-1}} \right]$$

La relation (2) devient maintenant

$$I(a_0, a_1, x_0+1, y_0) = \psi(a_0, a_1, y_0) - \psi(a_0, a_1, x_0) - I(a_1, a_2, x_1+1, y_1) \quad (3)$$

d'où, en désignant par  $k$  la longueur de l'algorithme d'Euclide du couple  $(a_0, a_1)$ , (ie  $a_k = (a_0, a_1) = 1$ ), nous tirons les égalités suivantes

$$I(a_0, a_1, x_0+1, y_0) = \psi(a_0, a_1, y_0) - \psi(a_1, a_2, y_1) \\ - (\psi(a_0, a_1, x_0) - \psi(a_1, a_2, x_1)) + I(a_2, a_3, x_2+1, y_2)$$

etc...

puis

$$I(a_0, a_1, x_0+1, y_0) = \psi(a_0, a_1, y_0) - \psi(a_1, a_2, y_1) + \dots + (-1)^{k-1} \psi(a_{k-1}, a_k, y_{k-1}) \\ - (\psi(a_0, a_1, x_0) - \psi(a_1, a_2, x_1) + \dots + (-1)^{k-1} \psi(a_{k-1}, a_k, x_{k-1}))$$

puisque on a toujours l'égalité  $I(a_k, 0, x, y) = 0$ .

Introduisons la fonction primitive d'une droite discrète

$$H(a_0, a_1, x_0) = \sum_{i=0}^{k-1} (-1)^i \psi(a_i, a_{i+1}, x_i),$$

l'intégrale s'exprime, en supprimant les indices de  $x$  et  $y$ , tout simplement comme une variation de la primitive discrète:

$$I(a_0, a_1, x+1, y) = H(a_0, a_1, y) - H(a_0, a_1, x) \quad (4)$$

Cette relation se généralise assez facilement si nous remplaçons le rationnel  $\frac{a_1}{a_0}$  par un nombre irrationnel  $\xi$ , la somme finie  $H$  devenant une série.

La relation (4) donne une évaluation exacte du nombre de points entiers positifs vérifiant l'inégalité  $ax+by \leq n$  contrairement aux formules approchées classiques de Césaro, Ramanujan et Hardy. Il reste à relier (4) à ces formules asymptotiques; ce qui sera fait dans un article suivant.

Pour des raisons algorithmiques nous pouvons chercher à évaluer le plus simplement possible les différentes bornes d'intégration  $x_i$  et  $y_i$  intervenant dans ces calculs en fonction des données  $a, b, x$  et  $y$ . Ceci nous amène à introduire les deux suites euclidiennes suivantes

$$a_0, a_1, a_2 = \left\{ \frac{a_0}{a_1} \right\}, \dots, a_{k+1} = \left\{ \frac{a_{k-1}}{a_k} \right\}, \dots$$

et

$$b_0, b_1, b_2 = \left\{ \frac{b_0}{b_1} \right\}, \dots, b_{k+1} = \left\{ \frac{b_{k-1}}{b_k} \right\}, \dots$$

où  $\frac{a_1}{a_0}$  est une nouvelle notation du rationnel  $\frac{a}{b}$  précédent et  $\frac{b_1}{b_0}$  est l'avant dernière réduite de  $\frac{a}{a_0}$ . Le théorème suivant donne une expression simple des diverses bornes d'intégration cherchées:

### Théorème 1

La suite  $\alpha_k = -\left\{ \frac{a_{k-1}}{a_k} \right\}^{-1} = -a_{k+1}^{-1} \pmod{a_k}$  définie pour  $k \geq 1$  (et  $\alpha_0 = 0$ ), est donnée par les égalités

$$\alpha_k = \begin{cases} a_k - b_k & \text{si } k \text{ est impair} \\ b_k & \text{si } k \text{ est pair.} \end{cases}$$

Intéressons nous maintenant aux sommes

$$S(b, a, i_0, i_1) = \sum_{i_0 \leq i \leq i_1} \left\{ \frac{ai}{b} \right\} \quad (5)$$

La fonction  $S$  étant périodique de période  $b$  en  $i_0$  ou  $i_1$ , nous pouvons supposer  $0 \leq i_1 - i_0 < b$ , ce qui nous ramène à un nombre de calculs inférieur à  $b$ , ceux des sommes  $S(b, a, 0, dn)$  avec  $0 \leq dn < b$ . Bien que ces calculs ne soient pas très complexes, surtout dans les applications informatiques, nous pouvons néanmoins les évaluer directement en fonction des entiers  $a$ ,  $b$  et  $dn$ .

Un calcul analogue au précédent fait apparaître la fonction rationnelle

$$\phi(b, a, x) = \frac{1}{2a} \left( (a+b-2)ax - (b-2) \left\{ \frac{ax}{b} \right\} + \left\{ \frac{ax}{b} \right\}^2 \right)$$

à l'aide de laquelle la somme  $S(b, a, x+1, y)$  vérifie l'égalité

$$S(b, a, x+1, y) = \phi(b, a, y) - \phi(b, a, x) - \frac{b}{a} S\left(a, \left\{ \frac{b}{a} \right\}, \alpha + \left[ \frac{ax}{b} \right] + 1, \alpha + \left[ \frac{ay}{b} \right] \right) \quad (6)$$

$\alpha$  étant encore le même que ci-dessus.

Cette dernière égalité fait encore intervenir la suite d'entiers  $b$ ,  $a$ ,  $\left\{ \frac{b}{a} \right\}, \dots$  constituée par les restes de l'algorithme d'Euclide du couple  $(b, a)$  (ou le développement en fraction continue de  $\frac{a}{b}$ ). Nous pouvons également

remplacer, comme ci-dessus, respectivement b et a par  $x_0$  et  $x_1$  et introduire les mêmes suites  $x_i$  et  $y_i$  pour les bornes de l'intervalle de sommation. Appliquons itérativement la formule (6), les égalités suivantes apparaissent:

$$\begin{aligned}
 S(a_0, a_1, x_0+1, y_0) &= \\
 &= \phi(a_0, a_1, y_0) - \phi(a_0, a_1, x_0) - \frac{a_0}{a_1} S(a_1, a_2, x_1+1, y_1) \\
 &= \phi(a_0, a_1, y_0) - \frac{a_0}{a_1} \phi(a_1, a_2, y_1) \\
 &\quad - (\phi(a_0, a_1, x_0) - \frac{a_0}{a_1} \phi(a_1, a_2, x_1)) + \frac{a_0}{a_2} S(a_2, a_3, x_2+1, y_2) \\
 &= \phi(a_0, a_1, y_0) - \frac{a_0}{a_1} \phi(a_1, a_2, y_1) + \frac{a_0}{a_2} \phi(a_2, a_3, y_2) \\
 &\quad - (\phi(a_0, a_1, x_0) - \frac{a_0}{a_1} \phi(a_1, a_2, x_1) + \frac{a_0}{a_2} \phi(a_2, a_3, x_2)) \\
 &\quad - \frac{a_0}{a_3} S(a_3, a_4, x_3+1, y_3)
 \end{aligned}$$

Finalement, si nous posons

$$\Theta(a_0, a_1, x_0) = \phi(a_0, a_1, x_0) - \frac{a_0}{a_1} \phi(a_1, a_2, x_1) + \dots + (-1)^k \frac{a_0}{a_k} \phi(a_k, a_{k+1}, x_k)$$

où  $a_k=1$  ( $=a_0, a_1$ ) et  $a_{k+1}=\dots=a_1=\dots=0$  pour  $i \geq k+1$  nous obtenons la relation suivante exprimant entièrement la somme (5):

$$S(a_0, a_1, x_0+1, y_0) = \Theta(a_0, a_1, y_0) - \Theta(a_0, a_1, x_0) \tag{7}$$

et ramenant l'évaluation de (5) au calcul de deux sommes ayant environ  $\log(a_1)$  termes.

## 2 Les points d'un réseau dans un rectangle isothétique.

Abordons la très ancienne question du dénombrement des points entiers contenus dans un domaine généralement convexe et rationnel. Le théorème de Pick apporte une réponse si les sommets du domaine sont également entiers mais ne s'applique pas s'ils sont rationnels. Dans le cas général les meilleurs résultats sont ceux d'Ehrhart (cf [40]); mais ils sont encore asymptotiques (voir [30] pour une description simple des méthodes d'Ehrhart). Nous donnons ici les premières formules exactes pour de tels dénombrements; pour alléger la présentation et aussi parce que ce cas présente déjà un intérêt pratique nous nous contentons d'évaluer le nombre de points entiers d'un parallélogramme

rationnel. Pour des raisons de commodité (discrétisation plus claire) nous étudions le problème équivalent de recherche du nombre de points d'un réseau entier (sous-groupe de  $\mathbb{Z}^2$ ) dans un rectangle isothétique à sommets entiers. Ce résultat permet par exemple de dénombrer les points d'une intersection de droites discrètes; de plus il devrait se généraliser à un convexe quelconque.

Soit  $\mathcal{R} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  un réseau entier réduit, ie les entiers  $a, b, c, d$  vérifient les conditions suivantes:

$$\begin{aligned} (a,b)=(b,d)=(c,d)=(a,c)=1 \\ ab-bc > 0 \end{aligned} \quad (1)$$

Nous voudrions déterminer le nombre de points de  $\mathcal{R}$  contenus dans le rectangle isothétique défini par les points  $(x_1, y_1)$  et  $(x_2, y_2)$  comme ci-dessous.

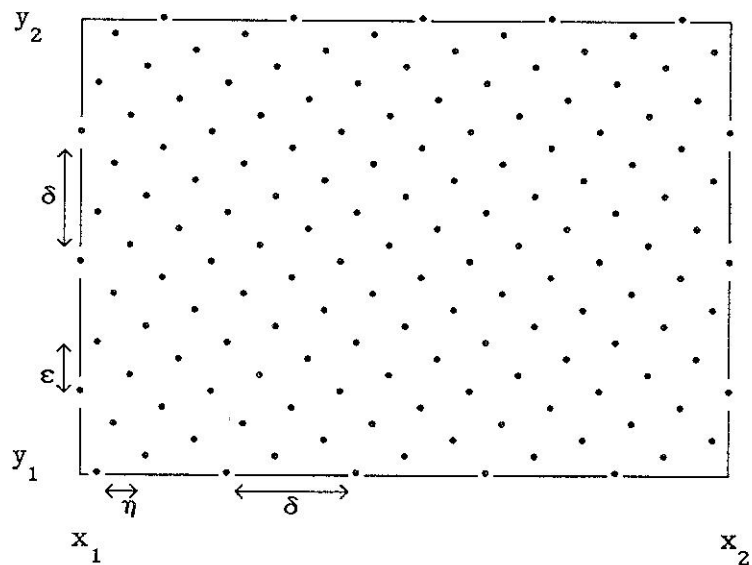


fig. 3

Nous commençons par faire quelques remarques tout en introduisant quelques quantités et notations utiles.

L'hypothèse (1) implique que toute parallèle à l'un des axes contient des points de  $\mathcal{R}$  périodiquement espacés de période  $\delta = ad-bc$ .

Nous appelons déphasage vertical la quantité  $\epsilon = \inf \{y | (1,y) \in \mathcal{R} \text{ et } y > 0\}$  et déphasage horizontal la quantité  $\eta = \inf \{x | (x,1) \in \mathcal{R} \text{ et } x > 0\}$ . D'après Bezout l'ensemble des couples d'entiers  $(u,v)$  pour lesquels  $au+bv=1$  est bien défini et paramètre l'ensemble des points de  $\mathcal{R}$  d'abscisse 1. Les ordonnées de ces points valent  $cu+dv$ . Donc nous avons

$$\epsilon = \left\{ \frac{cu+dv}{\delta} \right\}$$

où, deux entiers  $u$  et  $v$  étant donnés, nous désignons par  $\left\{ \frac{u}{v} \right\}$  le reste de la division de  $u$  par  $v$ . De même si  $az+bw = 1$  nous avons

$$\eta = \left\{ \frac{az+bw}{\delta} \right\}$$

Considérons une droite D d'équation  $X=x_0$  où  $x_0$  est entier. La distance à D des point  $(x,y) \in \mathcal{R}$  vérifiant  $|x-x_0| < \delta$ , peut également être évaluée en fonction de leur ordonnée  $y$ ; elle est donnée par  $\left\{ \frac{\eta y - x_0}{\delta} \right\}$  si  $x \geq x_0$  et par  $\left\{ \frac{x_0 - \eta y}{\delta} \right\}$  si  $x < x_0$ .

Désignons par  $N(\mathcal{R}, x_1, x_2, y_1, y_2)$  le nombre de points de  $\mathcal{R}$  dans le rectangle isothétique s'appuyant sur les sommets  $(x_1, y_1)$  et  $(x_2, y_2)$  bords compris. Notons que le nombre de points de  $\mathcal{R}$  situés dans un segment horizontal  $[x_1, x_2]$  est égal à l'entier

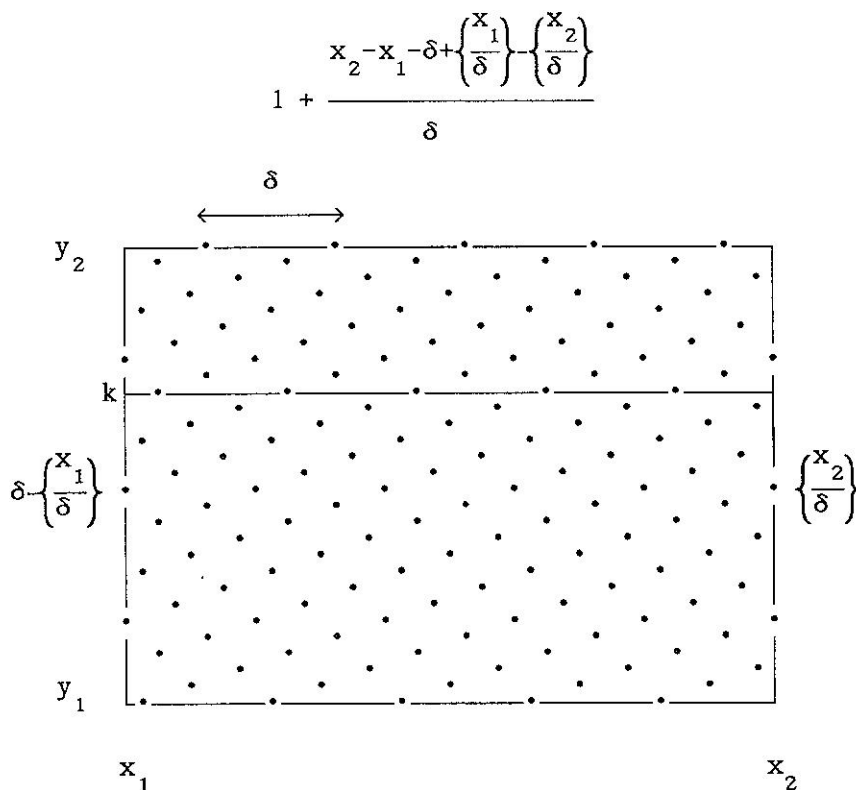


fig. 4

Le nombre de points de  $\mathcal{R}$  situés sur la droite d'ordonnée  $k$ , entre les points d'abscisse  $x_1$  et  $x_2$  est donc

$$1 + \frac{x_2 - x_1 + \left\{ \frac{k\eta - x_1}{\delta} \right\} - \left\{ \frac{x_2 - k\eta}{\delta} \right\}}{\delta}$$

Nous en déduisons l'expression suivante de  $N(\mathcal{R}, x_1, x_2, y_1, y_2)$ ,

$$N(\mathcal{R}, x_1, x_2, y_1, y_2) = 1 + y_2 - y_1 + \frac{(x_2 - x_1)(y_2 - y_1 + 1) - \sum_{k=y_1}^{k=y_2} \left[ \left\{ \frac{k\eta - x_1}{\delta} \right\} + \left\{ \frac{x_2 - k\eta}{\delta} \right\} \right]}{\delta} \quad (2)$$

Cette expression que nous allons modifier peu à peu, donne, dans tous les cas de figure le nombre de points du réseau  $\mathcal{R}$  dans le rectangle isothétique défini par les points entiers  $(x_1, y_1)$  et  $(x_2, y_2)$ .

Notre première réduction consiste à remarquer que la somme  $\sum_{k=y_1}^{k=y_2} \left\{ \frac{x_2 - k\eta}{\delta} \right\}$  est égale, pour une valeur  $\phi_2$  bien choisie, à la somme  $\sum_{k=\phi_2}^{y_2 - y_1 + \phi_2} \left\{ \frac{k\eta}{\delta} \right\}$ . De même il

existe une valeur entière  $\phi_1$  pour laquelle nous avons l'égalité

$$\sum_{k=y_1}^{k=y_2} \left\{ \frac{k\eta - x_1}{\delta} \right\} = \sum_{k=\phi_1}^{y_2 - y_1 + \phi_1} \left\{ \frac{k\eta}{\delta} \right\}. \text{ Les valeurs } \phi_1 \text{ et } \phi_2 \text{ sont données par les formules}$$

ci-dessous:

$$\phi_1 = \left\{ \frac{y_1 - \varepsilon x_1}{\delta} \right\}$$

et

$$\phi_2 = \left\{ \frac{\varepsilon x_2 - y_2}{\delta} \right\}.$$

Les valeurs  $\phi_1$  et  $\phi_2$  sont des cas particuliers de l'évaluation de la fonction  $\Phi$  définie comme suit:

pour tout point  $M(x, y)$  de  $\mathbb{Z}^2$  nous désignons par  $\Phi(x, y)$  la distance de  $M$  aux points de  $\mathcal{R}$  d'abscisse  $x$  et d'ordonnée  $\leq y$ . Il est facile de montrer que l'on a la relation

$$\Phi(x, y) = \left\{ \frac{y - \varepsilon x}{\delta} \right\}$$

Le calcul de  $N(\mathcal{R}, x_1, x_2, y_1, y_2)$  nous conduit donc à l'évaluation des sommes

$$S(b, a, S, T) = \sum_{k=S}^{k=T} \left\{ \frac{a + k}{b} \right\}$$

avec lesquelles la fonction  $N$  s'écrit

$$N(\mathcal{R}, x_1, x_2, y_1, y_2) = 1 + y_2 - y_1 + \frac{(x_2 - x_1)(y_2 - y_1 + 1) - S(\delta, \varepsilon, \phi_1, \phi_1 + y_2 - y_1) - S(\delta, \varepsilon, \phi_2, \phi_2 + y_2 - y_1)}{\delta}$$

La périodicité du réseau permet, avec une division euclidienne, de réduire la somme  $S(\delta, \varepsilon, y_1, y_2)$  à l'expression

$$\left[ \frac{y_2 - y_1}{\delta} \right] S(\delta, \varepsilon, 0, \delta - 1) + S\left(\delta, \varepsilon, y_1, y_1 + \left\{ \frac{y_2 - y_1}{\delta} \right\}\right)$$

Par conséquent le calcul d'une somme  $S(b, a, n, n + dn)$  se ramène toujours à une évaluation où  $0 \leq dn < b$ . L'évaluation est alors complète si nous faisons appel à la formule (7) du paragraphe précédent.

### Application numérique

Considérons le réseau  $\mathcal{R} \begin{pmatrix} 2 & -1 \\ 1 & 3 \end{pmatrix}$  et le rectangle isothétique défini par  $M_1(8,5)$  et  $M_2(25,21)$ . Les valeurs nécessaires au dénombrement par la formule précédente sont les suivantes

$$\delta = 7$$

$$u = 1, v = 1$$

$$z = -2, z = 1$$

$$\varepsilon = 4, \eta = 2$$

$$\phi_1 = 1, \phi_2 = 2$$

$$x_2 - x_1 = 4, y_2 - y_1 = 4,$$

$$S(\delta, \varepsilon, 0, \delta - 1) = 21,$$

cette dernière somme étant évaluée à la main; nous en déduisons

$$N(\mathcal{R}, M_1, M_2) = 17 + \frac{17 \cdot 17 - S(7, 2, 1, 17) - S(7, 2, 2, 18)}{7}$$

puis, en effectuant encore un calcul à la main, nous avons

$$S(7, 2, 1, 17) = 2 \times 21 + S(7, 2, 1, 3) = 42 + 12 = 54$$

et

$$S(7, 2, 2, 18) = 42 + S(7, 2, 2, 4) = 42 + 11 = 53$$

d'où il vient finalement le nombre de points recherchés

$$\begin{aligned} N(\mathcal{R}, M_1, M_2) &= 17 + \frac{289 - 107}{7} = 17 + \frac{182}{7} \\ &= 43. \end{aligned}$$

### 3 Droites discrètes et résidus quadratiques.

Indiquons dans ce paragraphe comment les droites discrètes sont reliées aux résidus quadratiques. Un célèbre **lemme de Gauss** exprime,  $p$  étant premier, le symbole de Legendre

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un résidu quadratique de } p, \\ -1 & \text{si } a \text{ est non résidu quadratique de } p, \\ 0 & \text{si } p \text{ divise } a, \end{cases}$$

sous la forme  $\left(\frac{a}{p}\right) = (-1)^\mu$  où  $\mu$  est le nombre des éléments de la forme

$$a, 2a, \dots, \left(\frac{p-1}{2}\right)a$$

dont les plus petits restes modulo  $p$  sont **négatifs**.

La variante de la division euclidienne, dite **au plus petit reste**, est, pour deux entiers  $a$  et  $p$  définie par l'égalité

$$a = pq + r \text{ où } r \in [-p/2], [p/2].$$

Il est alors clair que:

La droite de Bresenham associée à la droite  $y = \frac{a}{p}x$  est définie par  $y = \left[\frac{a}{p}x\right]^*$ , où  $\left[ \right]^*$  désigne le quotient au plus petit reste.

Sachant que la droite de Bresenham est aussi  $\mathcal{D}(a, -p, -[\frac{p}{2}], p)$  nous voyons que

*L'entier  $\mu$  est égal au nombre de points d'intersection de la droite naïve  $\mathcal{D}(a, -p, 0, p)$  et de la droite de Bresenham  $\mathcal{D}(a, -p, -[\frac{p}{2}], p)$  dont l'abscisse est comprise entre 1 et  $[p/2]$ .*

On en déduit aussitôt:

L'entier  $\mu$  est égal au nombre de points de l'intervalle  $[0, [\frac{p}{2}]]$  où

les fonctions  $\left[\frac{ax}{p}\right]$  et  $\left[\frac{ax + [\frac{p}{2}]}{p}\right]$  diffèrent de 1.

Ceci équivaut à:

L'entier  $\mu$  est égal au nombre de points de la droite  $\mathcal{D}(a, -p, 0, 1 + [\frac{p}{2}])$  contenus dans l'intervalle  $[1, [\frac{p}{2}]]$ .

Exemple:

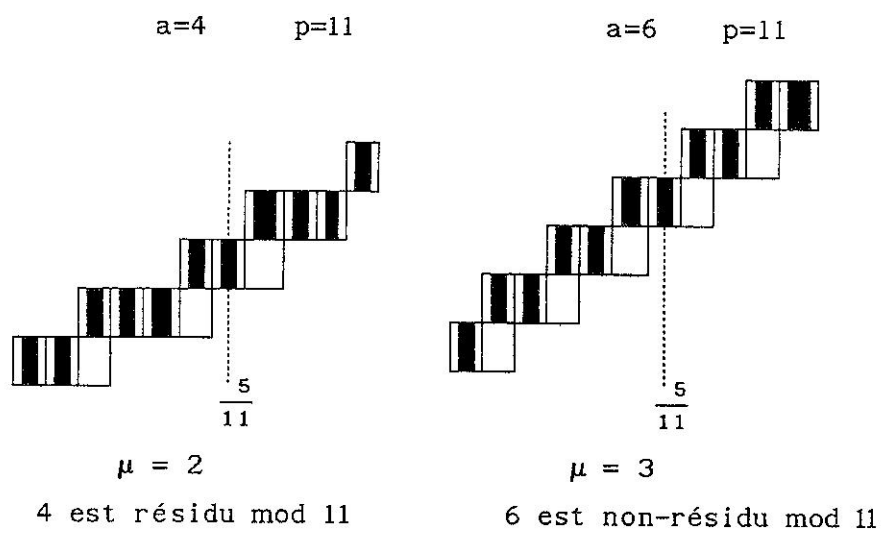


fig. 5

INTERSECTION DES DROITES DISCRETES

## INTRODUCTION

C'est dans leurs propriétés d'intersection que les droites discrètes se distinguent le plus des droites classiques. Comme la notion de droite discrète est liée à celle de bande "épaisse" le problème de leur intersection n'a rien à voir avec la troncature de l'intersection de deux droites réelles; c'est vers l'étude des points entiers des polygones plans, bornés ou non, qu'il faut se tourner. Nous nous retrouvons ainsi à proximité du vieux problème des partitions d'un entier en somme de formes linéaires non négatives (cf. Frobenius [], Brauer [9], Nijenhuis et Wilf [75]...), de celui de la détermination algorithmique des solutions d'équations diophantiennes linéaires (Clausen et Fortenbacher [23]) et inévitablement des questions de programmation linéaire entière; la question de l'intersection possède toutefois sa propre personnalité ce qui ne permet pas de la réduire tout simplement à ces questions.

Dans la section précédente la difficulté de l'approche analytique de la Géométrie Discrète a d'ailleurs déjà été évoquée; complétons un peu cet aspect des relations entre nombre et droite. Pour deux droites naïves de pentes  $\frac{a}{b}$  et  $\frac{c}{d}$ , initialisées par des valeurs des restes respectives de  $\varepsilon$  et  $\eta$  la recherche de leurs points d'intersection revient à la résolution de l'équation

$$\left[ \frac{ax+\varepsilon}{b} \right] = \left[ \frac{cx+\eta}{d} \right]$$

ou de l'équation modulaire équivalente

$$(ad-bc)x+d\varepsilon-b\eta = d \left\{ \frac{ax+\varepsilon}{b} \right\} - b \left\{ \frac{cx+\eta}{d} \right\}.$$

Ces équations, qui ne semblent pas attaques directement par voie analytique, résument bien ce problème d'intersection.

Les propriétés d'intersection des droites discrètes et euclidiennes diffèrent donc totalement. Dans le cas discret ces intersections peuvent non seulement contenir une infinité de points (droites parallèles pas encore confondues), mais aussi ne pas être connexes ou aller jusqu'à être vides. La portée de la Géométrie Discrète dépend essentiellement des réponses à ces questions et surtout de la façon dont elle répond: si la complexité de l'intersection de deux droites discrètes est une fonction des paramètres trop rapidement croissante nous ne pourrions pas en faire un usage intensif. Cette question n'a pas vraiment été abordée en Informatique Graphique; seul

l'article de Pham [83], propose un algorithme de parcours balayant systématiquement les deux droites.

Nous donnons, pour l'intersection, un algorithme de parcours fondé sur les réseaux, une méthode de réduction utilisant les opérateurs unimodulaires et des formules explicites de dénombrement fondées sur l'intégration discrète précédente. Il est remarquable que l'algorithme se réduise à un parcours de droite (pour un nouveau rationnel); sa complexité est donc celle du parcours d'une droite discrète. Par contre le chemin qui y conduit demande d'utiliser véritablement la Géométrie Discrète.

Nous donnons aussi, toujours pour l'intersection de deux droites, les conditions de non vacuité, celles de connexité et commençons l'étude des nombreuses questions liées à ses composantes connexes, (au sens des 4 ou 8 topologies).

Terminons cette introduction à l'étude de l'intersection des droites discrètes en signalant que leur irrégularité n'en n'est pas une si la regarde comme fonction de l'angle que font les deux droites. Dans le cas euclidien son comportement est discontinu: l'intersection est presque toujours un point puis, subitement, c'est la droite elle-même. Dans le cas discret c'est différent, l'intersection croît progressivement lorsque l'angle tend vers zéro. De plus nous savons que ces pathologies disparaissent "vues de loin", i.e. dans la Géométrie Discrète Idéale; c'est à dire si nous utilisons les entiers infiniment grands.

## I INTERSECTIONS ENTIERES ET INTERSECTIONS RATIONNELLES.

Comme les droites discrètes sont les solutions d'une double inégalité diophantienne, leur intersection revient à décrire l'ensemble des solutions entières (x,y) de quatre inéquations du type

$$\begin{aligned} \omega &\leq ax+by < \omega+\varepsilon \\ \rho &\leq cx+dy < \rho+\eta. \end{aligned} \tag{1}$$

Nous cherchons d'abord une solution algorithmique efficace au parcours de ce type d'ensembles en dégagant ses propriétés géométriques discrètes. Le partage de l'étude en deux cas, l'un particulier: l'intersection entière, l'autre général: l'intersection rationnelle, sera essentiel. Le premier est analogue aux droites dont l'épaisseur est un multiple de  $\sup(|a|, |b|)$ ,  $\frac{a}{b}$  étant la pente, i.e. droites qui sont réunion d'un nombre fini de droites 8-connexes; le deuxième cas correspond au cas générique des droites \*-connexes.

Si  $D$  et  $D'$  sont deux droites discrètes contenues dans deux bandes rationnelles  $B$  et  $B'$ , nous dirons que l'intersection de  $D$  et  $D'$  est entière si l'intersection des bords de  $B$  et  $B'$  est constituée de points entiers; sinon nous dirons que l'intersection est rationnelle. Avec les notations de (1) et en désignant par  $\delta = ad-bc$ , le déterminant, il est facile de vérifier

### Théorème 1

*L'intersection définie par (1) est entière si et seulement si l'on a les 4 conditions suivantes:*

$$\begin{cases} c\omega - a\rho \equiv 0 \pmod{\delta} \\ d\omega - b\rho \equiv 0 \pmod{\delta} \\ \varepsilon \equiv 0 \pmod{\delta} \\ \eta \equiv 0 \pmod{\delta} \end{cases}$$

Lorsque les deux dernières conditions seulement ( $\varepsilon \equiv 0$  et  $\eta \equiv 0 \pmod{\delta}$ ) sont vérifiées pour (1) nous dirons que les deux droites sont d'épaisseurs déterminantales, chacune étant divisible par le déterminant  $\delta$ . Là aussi le résultat suivant est clair

### Théorème 2

*Si  $D$  et  $D'$  sont d'épaisseurs déterminantales, l'intersection  $K = D \cap D'$  pave  $\mathbb{Z}^2$ .*

## II QUELQUES CAS PARTICULIERS

La classification précédente fait apparaître quelques cas particuliers intéressants.

### 1 Le cas des numérateurs consécutifs

Commençons par regarder le cas de l'intersection de deux droites naïves de pentes  $\frac{a}{b}$  et  $\frac{a-1}{b}$  passant par l'origine. Désignons par  $D(\frac{a}{b})$  et  $D(\frac{a-1}{b})$  ces deux droites. Le système (1) s'écrit

$$0 \leq ax + by < b \tag{2}$$

$$0 \leq (a-1)x + by < b$$

et comme le déterminant  $\delta$  vaut  $b$  nous sommes dans un cas d'intersection entière. Nous désignons encore par  $\mathcal{R}(\frac{a}{b})$  le réseau des restes associé à  $D(\frac{a}{b})$ .

En considérant les suites des restes de chacune d'elles, c'est à dire les

suites  $\left\{ \frac{ai}{b} \right\}$  et  $\left\{ \frac{(a-1)i}{b} \right\} = \left\{ \frac{ai-i}{b} \right\}$  nous pouvons faire les remarques suivantes.

o Les points de  $D(\frac{a}{b})$  dont le reste correspondant est un élément de  $\mathcal{R}(\frac{a}{b})$  situé au dessus de la diagonale, (dans le carré  $[0, b]^2$ ) sont également dans  $D(\frac{a-1}{b})$ ; la soustraction de  $i$  ne provoque pas de report de retenue.

o Les points de  $D(\frac{a}{b})$  dont le reste associé est sous la diagonale du carré  $[0,b]^2$  sont diminués d'une unité si on retranche  $i$  à leur reste. Dans ce cas les points de  $D(\frac{a}{b})$  sont juste au dessus de ceux de  $D(\frac{a-1}{b})$ . Par conséquent les points de  $D(\frac{a}{b})$  dont les restes sont en dessous de la diagonale du carré  $[-b,0] \times [0,b]$  sont aussi dans la droite  $D(\frac{a-1}{b})$ .

o Si nous désignons par  $\rho$  le parallélogramme engendré par les vecteurs  $(-b,0)$  et  $(b,b)$ , nous pouvons vérifier que les points de  $\mathcal{R}(a,b)$  qu'il contient sont en bijection avec ceux de  $D(\frac{a}{b}) \cap D(\frac{a-1}{b})$ . Nous venons de constater que tous ces points sont en correspondance avec des points de l'intersection; en fait ce sont les seuls.

o En effet la transformation  $\mathbb{Z}^2 \rightarrow \mathbb{Z}^2$  définie par l'opérateur

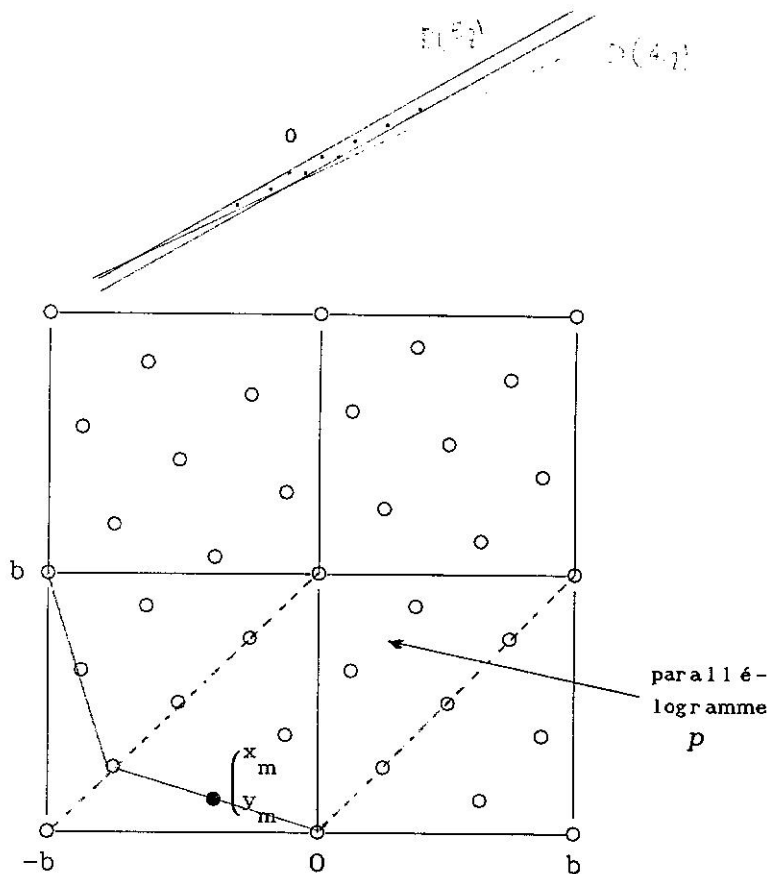
$$\begin{pmatrix} 1 & 0 \\ a & -b \end{pmatrix}$$

applique

$\mathbb{Z}^2$  sur  $\mathcal{R}(\frac{a}{b})$ ,

$D(\frac{a}{b})$  sur les points de  $\mathcal{R}(\frac{a}{b})$  d'ordonnée inférieure à  $b$ ,

$D(\frac{a-1}{b})$  sur les points de  $\mathcal{R}(\frac{a}{b})$  contenus dans la bande délimitée par les droites  $y=x$  (première bissectrice) et  $y=x+b$ . Comme l'intersection de ces deux bandes est le parallélogramme  $\rho$  l'assertion est vérifiée.



Intersection de deux droites discrètes.  
Cas des numérateurs consécutifs.

Fig. 1

Donnons quelques résultats supplémentaires de cette situation.

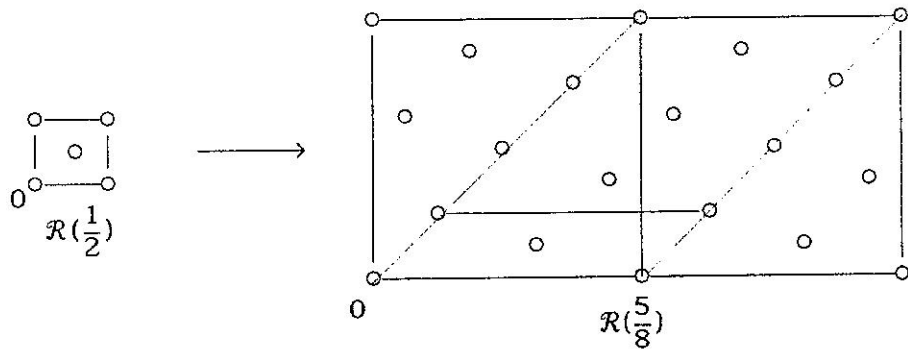
- 1 On trouve  $(a-1, b)$  points de  $\mathcal{R}(\frac{a}{b})$  sur la diagonale du carré  $[0, b]^2$ .
- 2 Soit  $(x_m, y_m)$  le premier vecteur de l'enveloppe convexe  $\mathcal{C}$  qui vérifie  $x_m > y_m$ , alors

$$x_m - y_m = (a-1, b).$$

- 3 L'opérateur

$$\begin{pmatrix} (a-1, b) & 1 \\ 0 & 1 \end{pmatrix}$$

applique bijectivement les points de  $\mathcal{R}(\frac{a-1}{b})$  contenus dans le carré  $\rho = [0, \frac{b}{(a-1, b)}]^2$  sur ceux de  $\mathcal{R}(\frac{a}{b})$  contenus dans le parallélogramme défini par les vecteurs  $(\frac{b}{(a-1, b)}, \frac{b}{(a-1, b)})$  et  $(b, 0)$  (voir fig.2 ci-dessous).



Transformation entre les réseaux  $\mathcal{R}(\frac{a}{b})$  et  $\mathcal{R}(\frac{a-1}{b})$ .

$$a=5, b=8, (a-1, b)=4.$$

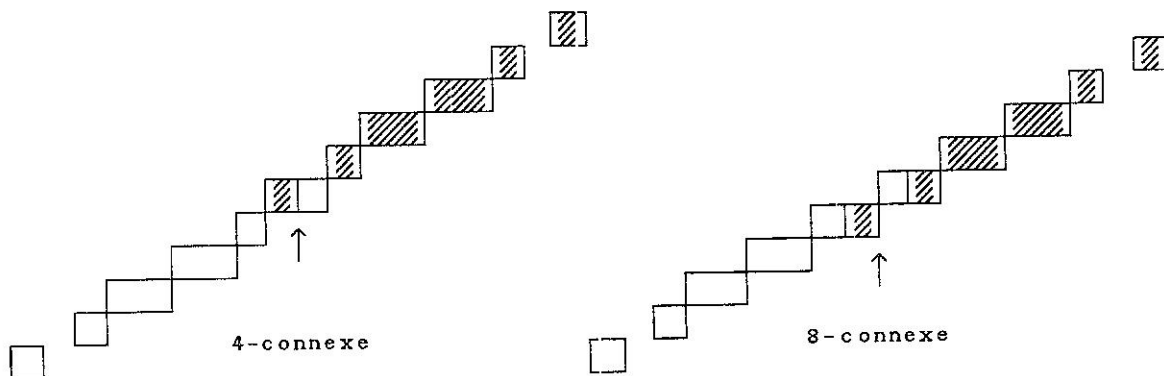
Fig. 2

Nous constatons que la description de l'intersection  $K=D(\frac{a}{b}) \cap D(\frac{a-1}{b})$  se ramène au parcours des points d'un réseau de restes,  $\mathcal{R}(\frac{a-1}{(a-1, b)}, \frac{b}{(a-1, b)})$ , que nous savons traiter efficacement.

Une autre conséquence intéressante apparaît alors. Comme  $\rho$  pave simultanément les sous-ensembles du réseau des restes  $\mathcal{R}(\frac{a}{b})$  contenus dans les bandes  $0 \leq y < b$  et  $0 \leq y-x < b$  nous obtenons

Corollaire

*L'intersection  $K=D(\frac{a}{b}) \cap D(\frac{a-1}{b})$  pave simultanément les droites  $D(\frac{a}{b})$  et  $D(\frac{a-1}{b})$ . Pour la première les divers exemplaires sont recollés de manière 4-connexe, pour la deuxième le recollement est 8-connexe.*



Les deux recollements d'un pavé K

Fig. 3

2 Le cas des numérateurs quelconques et des épaisseurs déterminantales.

Regardons comment se généralisent les résultats précédents pour de deux droites  $D(\frac{a}{b})$  et  $D(\frac{c}{b})$  où l'on a  $0 < c < a < b$  et  $(a,b)=1$ ,  $(b,c)$  quelconque et dont les épaisseurs sont égales à  $(a-c)b = \omega$ , déterminant du système. Désignons par  $D(a,b,\omega)$  et  $D(c,b,\omega)$  ces deux droites, respectivement définies par les inéquations diophantiennes

$$\begin{cases} 0 \leq ax - by < \omega \\ 0 \leq cx - by < \omega \end{cases} \quad (3)$$

C'est un cas d'intersection déterminantale. Il résulte de la propriété de pavage que les solutions de (3), qui sont également celles des équations

$$\begin{cases} \left[ \frac{ax - by}{\omega} \right] = 0 \\ \left[ \frac{cx - by}{\omega} \right] = 0 \end{cases}$$

sont, à translation près, celles de tous les systèmes

$$\begin{cases} \left[ \frac{ax - by}{\omega} \right] = k \\ \left[ \frac{cx - by}{\omega} \right] = \ell \end{cases}$$

où  $k$  et  $\ell$  sont entiers. Cette particularité se traduit en un parcours simple de l'ensemble de leurs solutions.

Une conséquence de cette propriété, analogue à celle du premier cas, est la suivante: sous ces conditions l'intersection  $D(\frac{a}{b}) \cap D(\frac{c}{b})$  pave simultanément l'une et l'autre droite.

Introduisons les couples d'entiers suivants:

$$(b', c') = \left( \frac{b}{(b,c)}, \frac{c}{(b,c)} \right)$$

$$(u, v) \text{ tel que } cu - bv = (b,c), u \in [0, b-1], \text{ est le vecteur de Bezout de } (b,c)$$

$$(s, t) = (b' - u, c' - v)$$

$$(\bar{a}, \bar{b}) = (au - bv, (a-c)b').$$

Théorème 3

Avec les notations précédentes, l'ensemble des solutions du système (1) est donné par  $(b,c)$  applications de l'algorithme des 2 vecteurs  $V_1 = (u,v)$ ,  $V_2 = (s,t)$  pilotés par le rationnel  $\frac{\bar{a}}{\bar{b}}$  à partir des points  $k(b',c')$  pour  $k=0, \dots, (b,c)-1$ .

Donnons quelques exemples et l'algorithme que nous pouvons tirer de ce théorème avant de regarder la démonstration; ils montreront sa simplicité et son intérêt.

$$1 \quad \frac{a}{\bar{b}} = \frac{7}{9}, \quad \frac{c}{\bar{b}} = \frac{5}{9}, \quad \text{d'où nous tirons:}$$

$$(b,c)=1, \quad b'=b=9, \quad c'=c=5,$$

$$V_1=(u,v)=(2,1),$$

$$V_2=-(s,t)=-(7,4),$$

$$\bar{a} = 2 \cdot 2 + 1 = 5, \quad \bar{b} = 18$$

La suite des restes  $\left\{ \frac{5i}{18} \right\}$  est

0 5 10 15 2 7 12 17 4 9 14 1 6 11 16 3 8 13

Cette liste nous donne la suite des incréments ( $V_1$  si la valeur n'est pas soulignée et  $V_2$  sinon) à ajouter au vecteur initial (0,0) pour obtenir toutes les solutions des inégalités

$$\begin{cases} 0 \leq 7x - 9y < 18 \\ 0 \leq 5x - 9y < 18. \end{cases}$$

La liste des solutions est par conséquent:

(0,0) (2,1) (4,2) (-1,-1) (1,0) (3,1) (5,2) (-2,-2) (0,-1) (2,0) (-5,-4)  
 (-3,-3) (-1,-2) (1,-1) (-6,-5) (-4,-4) et (-2,-3).

Nous pouvons représenter graphiquement cette intersection des deux droites

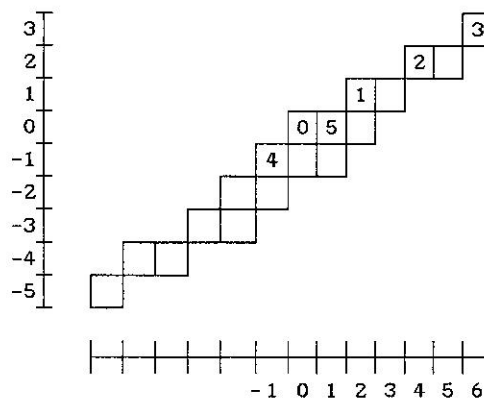


Fig. 4

sur laquelle nous avons fait figurer les premiers numéros du parcours.

La figure suivante donne une vue plus complète de l'intersection des deux droites correspondantes.

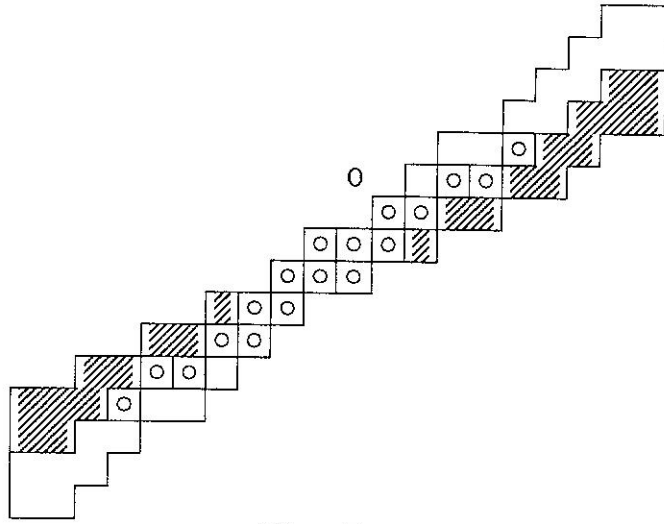


Fig. 5

$$\begin{aligned}
2 \quad \frac{a}{b} &= \frac{8}{15}, \quad \frac{c}{b} = \frac{6}{15}, \quad \text{d'où il vient:} \\
&(b,c)=3, \quad b'=5, \quad c'=2, \\
V_1 &=(u,v)=(3,1), \\
V_2 &=-(s,t)=-(2,1), \\
\bar{a} &= 2.3+3 = 9, \quad \bar{b} = 10
\end{aligned}$$

La suite des restes est: 0,9,8,7,6,5,4,3,2,1; le vecteur  $V_1=(3,1)$  est appliqué en 0 seulement et  $V_2 = -(2,1)$  pour toutes les autres valeurs. Par conséquent les solutions des inégalités

$$\begin{cases} 0 \leq 8x - 15y < 30 \\ 0 \leq 6x - 15y < 30, \end{cases}$$

s'obtiennent comme réunion de trois ensembles  $\mathcal{P} \cup \mathcal{P}' \cup \mathcal{P}''$  où  $\mathcal{P} = \{(0,0) (3,1) (1,0) (-1,-1) (-3,-2) (-5,-3) (-7,-4) (-9,-5) (-11,-6) (-13,-7)\}$ ,  $\mathcal{P}' = \mathcal{P} + (5,2)$  et  $\mathcal{P}'' = \mathcal{P} + 2.(5,2)$ . Leur représentation graphique comme intersection des droites discrètes correspondantes est donnée ci-dessous; les éléments de  $\mathcal{P}$  sont figurés avec un pixel marqué.

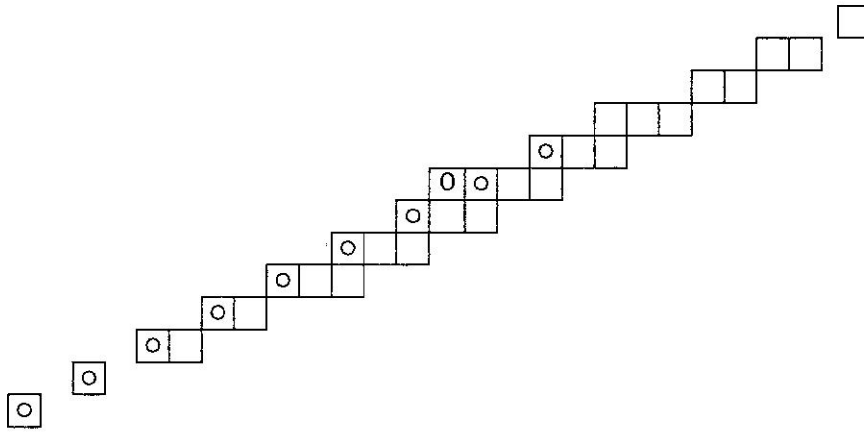


Fig. 6

$$\begin{aligned}
3 \quad \frac{a}{b} &= \frac{9}{16}, \quad \frac{c}{b} = \frac{6}{16}, \text{ d'où il vient:} \\
&(b,c)=2, \quad b'=8, \quad c'=3, \\
V_1 &=(u,v)=(3,1), \\
V_2 &=-(s,t)=-(5,2), \\
\bar{a} &= 3 \cdot 3 + 2 = 11, \quad \bar{b} = 24.
\end{aligned}$$

La suite des restes est ici égale à:

$$0, 11, \underline{22}, 9, \underline{20}, 7, \underline{18}, 5, \underline{16}, 3, \underline{14}, 1, \underline{12}, \underline{23}, 10, \underline{21}, 8, \underline{19}, 6, \underline{17}, 4, \underline{15}, 2, \underline{13};$$

nous avons souligné les éléments correspondant au vecteur  $V_2$ .

L'ensemble des solutions des inégalités

$$\begin{cases} 0 \leq 9x - 16y < 48 \\ 0 \leq 6x - 16y < 48, \end{cases}$$

est alors réunion de deux sous-ensembles  $\mathcal{P}$  et  $\mathcal{P}' = \mathcal{P} + (8,3)$ . Il suffit d'expliciter le premier; il est constitué de la suite de points entiers:

$$\begin{aligned}
\mathcal{P} &= \{(0,0), (3,1), (6,2), (1,0), (4,1), (-1,-1), (2,0), (-3,-2), (0,-1), (-5,-3), (-2,-2), \\
&(-7,-4), (-4,-3), (-1,-2), (-6,-4), (-3,-3), (-8,-5), (-5,-4), (-10,-6), (-7,-5), \\
&(-12,-7), (-9,-6), (-14,-8), (-11,-7)\}.
\end{aligned}$$

La représentation de l'intersection s'en déduit. Nous y avons fait figurer les points de  $\mathcal{P}$  avec des pixels surchargés; il apparaît nettement que  $\mathcal{P}'$  est bien le translaté de  $\mathcal{P}$  de vecteur  $(8,3)$ .

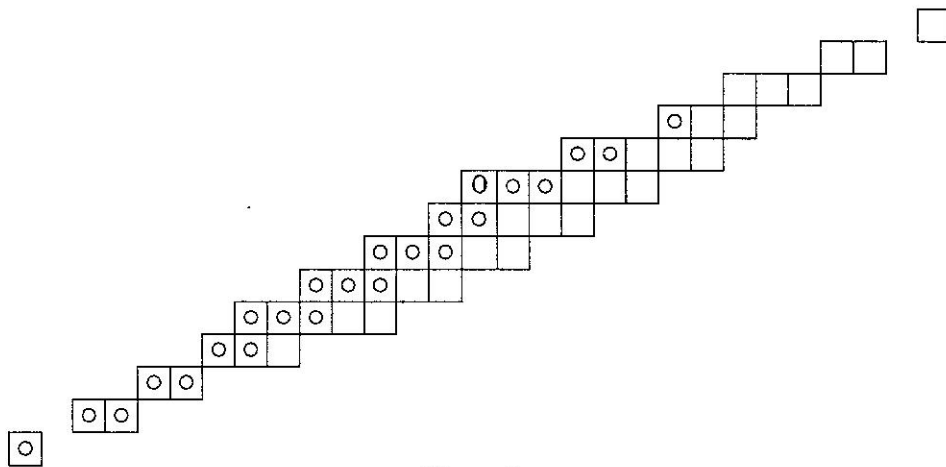


Fig. 7

Algorithme de parcours de l'intersection  $\mathcal{D}(\frac{a}{b}) \cap \mathcal{D}(\frac{c}{b})$ ;  
 Cas d'épaisseur  $(a-c)b$ .

Calculer  $(b,c)$ ,  $b'$ ,  $c'$ ,  $V_1=(u,v)$ ,  $V_2=-(s,t)$ ,  $\bar{a}$  et  $\bar{b}$ .

$X$  est le point courant de  $\mathbb{Z}^2$ ;  $T$  le début de chaque sous-ensemble de solutions.

$T=0$ ;

For  $i=1$  to  $(b,c)$  do

begin

$X=T$ ;  $r=0$ ;

for  $j=1$  to  $(a-c)b$  do

if  $r < (\bar{b}-\bar{a})$  then

begin

$r=r+\bar{a}$ ;  $X=X+V_1$

end

else

begin

$r=r-\bar{b}+\bar{a}$ ;  $X=X-V_2$

end;

$T=T+(b',c')$

end;

#### Remarques:

La condition d'épaisseur égale à  $(a-c)b$  assure que l'intersection, formée de  $(a-c)b$  points, est paramétrable par un simple parcours à 2 vecteurs pilotés par un rationnel. Ce n'est plus le cas si les épaisseurs des droites sont quelconques; la théorie des fenêtres euclidiennes et des parcours associés est alors nécessaire (et suffisante).

Dans ce cas particulier les droites passent par l'origine; comme nous l'avons déjà vu à plusieurs reprises un changement des conditions initiales provoque une translation de ces droites sans les modifier leur structure. Il suffit de déterminer les déphasages associés pour traiter ce cas.

Ce qui est illustré dans ces exemples est en fait générique, aux fenêtres euclidiennes près. Par conséquent la complexité du parcours d'une intersection est du même type que celle du parcours d'une droite discrète. De même tout algorithme rapide pour ce dernier problème s'adapte à l'intersection et améliore les performances de sa détermination; en particulier l'algorithme des

cas de palier par convexité. Ceci donne un très grand nombre de variantes possibles. Par souci de simplicité nous ne traiterons dans la suite que les aspects théoriques de l'intersection et ne donnerons que les versions les plus élémentaires des algorithmes de parcours. Nous laissons au lecteur intéressé le soin d'écrire les variantes dont il a besoin.

On constatera que le traitement du deuxième cas, abordé par la voie la plus naturelle possible, conduit à l'emploi de plusieurs transformations qui pourraient s'avérer fastidieuses dans l'étude du cas général; de surcroît les réseaux entiers ont montré leur utilité ici. Voici les raisons de traduire l'intersection en un problème de réseaux; ce sera le but du paragraphe suivant.

Intéressons-nous maintenant à la démonstration du théorème dont nous allons donner une preuve "géométrique" évitant autant que possible les calculs avec les quotients et les restes qui conduisent généralement à des impasses.

Le principe consiste à placer trois parallélogrammes sur le réseau des restes  $\mathcal{R}(\frac{a}{b})$  et à identifier les points du réseau contenus avec des suites de restes d'autres rationnels au moyen de transformations linéaires.

Désignons par  $\rho$  le parallélogramme construit sur les vecteurs  $(-b,0)$  et  $(b,(a-c)b)$ . Avec les mêmes raisonnements que dans le cas 1 on montre que les points de  $\mathcal{R}(\frac{a}{b}) \cap \rho$  sont en correspondance biunivoque avec ceux de l'intersection; (dans toute cette partie les parallélogrammes sont "fermés" le long des deux vecteurs qui les définissent et "ouverts" sur les deux autres côtés).

Soient  $\rho'$  le parallélogramme construit sur  $(b',(a-c)b')$  et  $(0,b)$  et  $\bar{\rho}$  celui construit sur  $(-b,0)$  et  $(b',(a-c)b')$ .

Les points de  $\mathcal{R}(\frac{a}{b}) \cap \rho'$  sont en correspondance avec les points de  $\mathcal{R}(\frac{c'}{b'})$  contenus dans le carré  $[0,b'[ \times ]0,b'[$  par la bijection

$$A: \mathcal{R}(\frac{c'}{b'}) \longrightarrow \mathcal{R}(\frac{a}{b})$$

$$(i, j) \longrightarrow \begin{pmatrix} 1 & 0 \\ a-c & (b, c) \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix}$$

Mais il est clair sur la figure que bien que  $\rho' \subset \rho$ , ce dernier n'est pas pavé par un nombre entier d'exemplaires de  $\rho'$ .

Par contre  $\rho$  est une réunion de  $(b,c)$  exemplaires du parallélogramme  $\bar{\rho}$ . C'est

le parallélogramme le plus adapté à la description de l'intersection; seulement il faut décrire l'ensemble des points de  $\mathcal{R}(\frac{a}{b}) \cap \bar{\rho}$  au moyen d'une suite arithmétique adéquate; autrement dit il faut exhiber un nouveau rationnel. En observant la figure nous constatons que  $\bar{\rho}$  contient  $(a-c)b'$  points; c'est le dénominateur  $\bar{b}$  du rationnel cherché. Nous pouvons appliquer canoniquement le carré  $[0, (a-c)b']^2$  sur  $\bar{\rho}$  par la transformation

$$B = \begin{pmatrix} \frac{(b,c)}{a-c} & \frac{1}{a-c} \\ 0 & 1 \end{pmatrix}$$

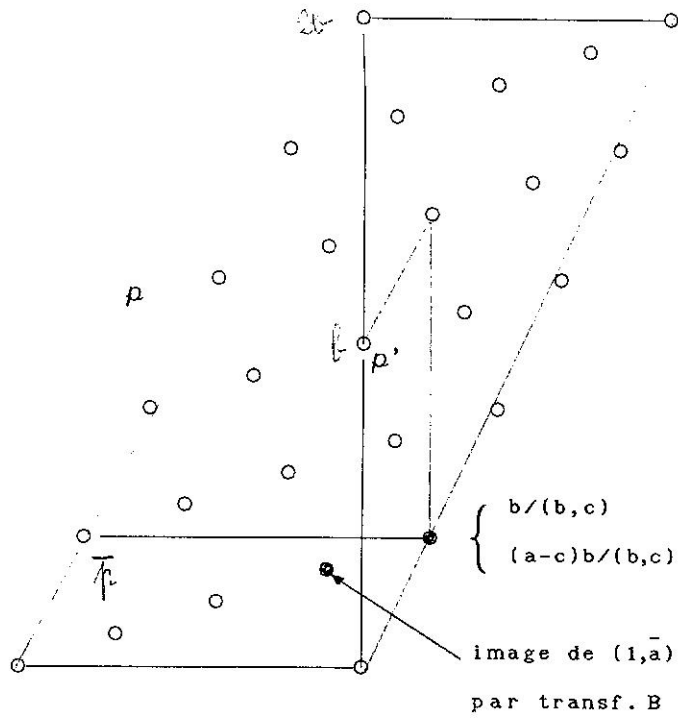
d'inverse

$$B^{-1} = \begin{pmatrix} \frac{(a-c)}{(b,c)} & \frac{1}{(b,c)} \\ 0 & 1 \end{pmatrix}.$$

Considérons maintenant le vecteur  $(c'^{-1}, 1)$  du réseau des restes  $\mathcal{R}(\frac{c'}{b})$ ,  $c'^{-1}$  étant calculé mod  $b'$ , i.e. il est défini comme l'unique vecteur de Bezout égal à la composante  $u$  de l'unique vecteur de Bezout  $(u, v)$  vérifiant

$$c'u - b'v = 1 \text{ et } u \in [0, b'[,$$

Par  $A$  ce vecteur devient  $(u, au - bv)$ ; en composant ensuite par  $B^{-1}$  nous obtenons:  $(1, au - bv)$ . Comme la première composante est nulle et comme l'entier  $\bar{a} = au - bv = (a-c)u + (b,c)$  est premier avec  $(a-c)b'$ , l'ensemble des points de  $\mathcal{R}(\frac{a}{b}) \cap \bar{\rho}$  peut être décrit par la suite des restes du rationnel  $\frac{\bar{a}}{\bar{b}}$ ; (nous prouvons plus loin l'assertion concernant  $\bar{a}$ ). Plus précisément  $\mathcal{R}(\frac{a}{b}) \cap \bar{\rho}$  est l'image des points du réseau des restes de  $\frac{\bar{a}}{\bar{b}}$  contenus dans  $[0, \bar{b}[^2$  par l'opérateur  $B$ .



$$\mathcal{D}\left(\frac{7}{10}\right) \cap \mathcal{D}\left(\frac{5}{10}\right), \quad (b, c) = 5,$$

$$\bar{a} = 3, \quad \bar{b} = 4.$$

Fig. 8

Ce qui nous intéresse en fait c'est le parcours de l'intersection des droites dans  $\mathbb{Z}^2$ . Or la transformation qui fait passer de la droite discrète  $\mathcal{D}\left(\frac{a}{b}\right)$  à son réseau des restes est donnée par l'opérateur

$$\mathcal{D}\left(\frac{a}{b}\right): \left[ \frac{ax-by}{w} \right] = 0 \longrightarrow \mathcal{R}\left(\frac{a}{b}\right)$$

$$(x, y) \longrightarrow \begin{pmatrix} 1 & 0 \\ a & -b \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

son inverse est donc  $\frac{1}{b} \begin{pmatrix} b & 0 \\ a-1 & 1 \end{pmatrix}$ . Il suffit de calculer l'image du vecteur

$(u, (a-c)u + (b, c))$  par cette transformation ainsi que celle du vecteur  $(b', (a-c)b')$ . Nous trouvons respectivement les vecteurs  $(u, v)$  et  $(b', c')$ . Nous en déduisons les vecteurs  $V_1 = (u, v)$ ,  $V_2 = -(b', c') + (u, v)$  que nous désignons par  $(s, t)$  et le vecteur  $(b', c')$  de translation du point initial de chaque tracé lorsque le pgcd  $(b, c)$  est supérieur à 1.

Le théorème s'en déduit. Prouvons maintenant le résultat  $(\bar{a}, \bar{b}) = 1$ .

lemme 1

*Les entiers  $\bar{a}=au-bv$  et  $\bar{b}=(a-c)b'$  sont premiers entre eux.*

On vérifie immédiatement l'égalité

$$c'\bar{a} - v\bar{b} = a \quad (2)$$

Les entiers  $a$  et  $b$  étant premiers entre eux, par hypothèse, il existe, d'après Bezout, deux entiers  $x$  et  $y$  tels que

$$ax - (a-c)b'y = (a,c)$$

En multipliant (2) par  $x$  et en y reportant  $ax$  tiré de la précédente égalité nous obtenons la relation

$$c'x\bar{a} - (vx+y)\bar{b} = (a,c). \quad (3)$$

Or  $(a,c)$  et  $\bar{a} = (a-c)u+(b,c)$  sont premiers entre eux, il existe, à nouveau par Bezout deux entiers  $x'$  et  $y'$  pour lesquels on a

$$x'(a,c) - y'\bar{a} = 1.$$

Tirons  $x'(a,c)$  de cette dernière et reportons le dans (3) multipliée par  $x'$ , il vient l'égalité de Bezout

$$(cxx'-y')\bar{a} - (vx+y)\bar{b} = 1$$

qui prouve l'assertion.

### III DROITES DISCRETES ET RESEAUX.

#### 1 Un réseau pour deux droites.

Pour toute matrice entière  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  nous désignons par  $\mathcal{R}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  le réseau engendré par les vecteurs  $\begin{pmatrix} a \\ c \end{pmatrix}$  et  $\begin{pmatrix} b \\ d \end{pmatrix}$  i.e. le sous-ensemble de  $\mathbb{Z}^2$  suivant

$$\mathcal{R}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \{(x,y) | x=ak+bl, y=ck+dl \ (k,l) \in \mathbb{Z}^2\}$$

Soit  $\mathcal{D}$  une droite discrète donnée par ses inéquations diophantiennes

$$(\mathcal{D}) \quad \{(x_0, y_0) | x_0, y_0 \in \mathbb{Z} \text{ et } s \leq ax_0 + by_0 < s'\}$$

où  $a, b, s$  et  $s'$  sont entiers. L'image de  $\mathcal{D}$  par toute transformation de  $\mathbb{Z}^2$  de matrice  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  où  $c$  et  $d$  sont entiers et  $\delta = ad - bc > 0$  est l'ensemble des points du réseau  $\mathcal{R}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  dont la première composante est comprise entre  $s$  et  $s'$ :  $s \leq ax + by \leq s'$ ; et cette image est en bijection avec  $\mathcal{D}$  tant que  $\delta \neq 0$ . Comme les deux paramètres  $c$  et  $d$  sont "libres" nous pouvons également les utiliser pour représenter simultanément une deuxième droite discrète. Soit  $\mathcal{E}$  une autre droite discrète

$$(\mathcal{E}) \quad = \quad \{(x_0, y_0) | x_0, y_0 \in \mathbb{Z} \text{ et } t \leq cx_0 + dy_0 < t'\}$$

elle est en bijection avec les points du réseau  $\mathcal{R}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  dont la deuxième composante  $cx + dy$ ,  $(x, y \in \mathbb{Z})$ , vérifie les contraintes  $t \leq cx + dy \leq t'$ . Nous avons donc le résultat suivant.

#### Théorème 1

*Soient  $\mathcal{D}$  et  $\mathcal{E}$  deux droites discrètes définies comme ci-dessus, l'ensemble de leurs points d'intersection est en correspondance bijective avec les points*

*$(x, y)$  du réseau  $\mathcal{R}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  vérifiant les inégalités  $s \leq x < s'$  et  $t \leq y < t'$ .*

Nous l'appellerons le "réseau des équations" des deux droites.

#### 2 Paramétrage de l'intersection de deux droites.

Nous déduisons de ce théorème un algorithme de construction des points de  $\mathcal{D} \cap \mathcal{E}$ . Son principe consiste à décrire les points de  $\mathcal{R}$  contenus dans le rectangle isothétique  $\text{Rec}(s, t, s', t')$  défini par les deux points  $(s, t)$  et  $(s', t')$  et à les appliquer, par la matrice  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$  sur l'intersection cherchée.

Nous supposons, ce qui est toujours possible via une transformation

évidente, que la matrice  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  vérifie les conditions  $(a,b)=(b,d)=(c,d)=(a,c)=1$ ; il en résulte qu'il existe des points de  $\mathcal{R}$  sur toutes les droites parallèles aux axes de coordonnées passant par les points entiers. De plus ces points sont disposés périodiquement la période étant  $\delta$ . Soit  $\varepsilon$  la constante entière définie par

$$\varepsilon = \inf \{y \mid (1,y) \in \mathcal{R} \text{ et } y > 0\}$$

et soit  $e(x,y)$  la fonction définie de manière analogue par

$$e(x,y) = \inf \{(z-y) \mid (x,z) \in \mathcal{R} \text{ et } z > y\}$$

c'est à dire la distance du point de  $\mathcal{R}$  le plus proche de  $(x,y)$  parmi ceux qui ont l'abscisse  $x$  et une ordonnée supérieure à  $y$ . Ces constantes s'expriment en fonction des données.

lemme 1

a) La constante  $\varepsilon$  du réseau  $\mathcal{R}$  est  $\varepsilon = \left\{ \frac{cm+dn}{\delta} \right\}$ ,  $m$  et  $n$  étant donnés par la relation de Bezout  $am+bn=1$ .

b) Nous avons  $e(x,y) = \left\{ \frac{x\varepsilon-y}{\delta} \right\}$ .

La périodicité mentionnée ci-dessus montre que la configuration des points de  $\mathcal{R}$  dans le rectangle isothétique  $\text{Rec}(s,t,s',t')$  est invariante si  $(s,t)$  et  $(s',t')$  sont translatés d'un même vecteur  $(k\delta, l\delta)$   $k, l \in \mathbb{Z}$ . Parmi les rectangles étudiés le cas des carrés  $s'-s=t'-t=\delta$  est particulièrement simple et permet de traiter ensuite tous les autres. Dans ce cas les points du réseau sont paramétrés par une suite arithmétique.

proposition 1

Les points de  $\mathcal{R} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  situés dans le carré  $\text{Rec}(0,0,\delta-1,\delta-1)$  sont donnés par la suite  $(i, \left\{ \frac{\varepsilon i}{\delta} \right\})$  où  $i \in [0, \delta-1]$ . Les points de  $\mathcal{R} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  situés dans le carré  $\text{Rec}(s,t,s+\delta-1,t+\delta-1)$  sont donnés par la suite  $(i, \left\{ \frac{e+\varepsilon i}{\delta} \right\})$  où  $e = e(s,t)$  et  $i \in [0, \delta-1]$ .

Dans un cas un peu plus général, si la fenêtre est  $\text{Rec}(0,0,k,h)$ , nous avons besoin de faire intervenir les bases euclidiennes du réseau. Par définition ce réseau est également engendré par la base  $(0,\delta), (1,\varepsilon)$ . Nous pouvons donc considérer les vecteurs euclidiens de ce réseau engendrés à partir de cette base par l'algorithme de Jacobi-Perron **additif** et en particulier les deux vecteurs  $U=(\kappa,\gamma)$  et  $U'=(\kappa',\gamma')$  consécutifs qui vérifient

les inégalités

$$\gamma' \geq h > \gamma.$$

Nous définissons maintenant les vecteurs  $A=(\alpha,\beta)$  et  $A'=(\alpha',\beta')$  suivants, dits vecteurs du parcours du réseau:

$$A = U, \quad A' = U-U' \quad \text{si } \kappa > 0,$$

et

$$A = U'-U, \quad A' = -U \quad \text{si } \kappa < 0.$$

Il est facile de vérifier que les ordonnées des points du réseau  $\mathcal{R} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  situés dans la fenêtre  $\text{Rec}(s,t,s+k,t+h)$  sont données par la suite arithmétique  $\left\{ \frac{\beta i}{\gamma} \right\}$  tronquée à la hauteur  $h$ . Nous obtenons alors un algorithme de parcours analogue à celui que nous avons déjà obtenu à la section 1. Comme nous nous intéressons essentiellement à ce qui se passe dans l'intersection nous donnons un algorithme qui parcourt directement les points de celle-ci.

Nous pouvons repasser du réseau  $\mathcal{R} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  aux coordonnées entières des points

des deux droites via l'opérateur  $M = \frac{1}{\delta} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$  (qui est à valeurs entières).

Si nous posons  $V=MA$  et  $V'=MA'$  et désignons par  $X=(x,y)$  le point courant dans l'intersection et  $p$  l'abscisse du point correspondant dans le réseau

$\mathcal{R} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , l'algorithme se met sous la forme suivante.

Algorithme d'intersection de deux droites.

```
X=0; p=0; r=0;
```

```
repeat
```

```
    afficher X;
```

```
    if  $r < h - \beta$  then begin  $p=p+\alpha$ ;  $r=r+\beta$ ;  $X=X+V$  end
```

```
    else if  $r < \gamma' - \beta$  then begin  $p=p+\alpha+\alpha'$ ;  $r=r+2\beta-\gamma'$ ;  $X=X+2V-V'$  end
```

```
        else begin  $p=p+\alpha'$ ;  $r=r+\beta-\gamma'$ ;  $X=X+V-V'$  end;
```

```
until  $p > k$ ;
```

Le cas le plus général réclame de déplacer la fenêtre sur le réseau et se ramène à adjoindre à cet algorithme celui qui détermine le "premier point" d'une fenêtre vu dans la section 1.

Donnons maintenant quelques exemples d'utilisation de cet algorithme.

$$1 \text{ Résolution des inéquations } \begin{cases} 0 \leq 2x-3y < 9 \\ 0 \leq 7x-4y < 9. \end{cases}$$

Le réseau des équations est  $\mathcal{R} \begin{pmatrix} 2 & -3 \\ 7 & -4 \end{pmatrix}$ ,  $\delta=13$ ,  $\varepsilon=10$ ; l'opérateur de retour est  $M = \frac{1}{13} \begin{pmatrix} -43 \\ -72 \end{pmatrix}$ . Les dimensions de la fenêtre sont  $k=9$  et  $h=9$ . Les vecteurs euclidiens  $U$  et  $U'$  engendrés à partir de  $(0,13)$  et  $(1,10)$  sont  $U'=(1,10)$  et  $U=(2,7)$ ; d'où, comme  $\kappa=2>0$ , les vecteurs de parcours du réseau des équations  $A=(2,7)$  et  $A'=(1,-3)$ . Ceux du parcours des droites sont  $V=(1,0)$  et  $V'=(-1,-1)$ . Le rationnel pilote est  $\frac{\beta}{\gamma} = \frac{7}{10}$ . La suite des restes  $\{\frac{7i}{10}\}$  tronquée par  $h=9$  est représentée ci-dessous à la ligne  $r$ . Nous y avons également fait figurer le vecteur déplacement,  $\Delta$ , dans l'intersection (leur somme est  $X$ ) et la variable de contrôle  $p$ . L'algorithme s'arrête dès que cette dernière dépasse la largeur  $k=9$  de la fenêtre; ici pour  $i=6$ . Nous devons donc effectuer, à partir de 0 les déplacements indiqués dans les colonnes allant de 0 à 5.

i	0	1	2	3	4	5	6
r	0	7	4	1	8	5	2
p	2	3	4	6	7	8	11
$\Delta$	V	V'	V'	V	V'	V'	

Remarquons que ce parcours est celui d'une suite arithmétique ordinaire; le fait que  $h$  soit une hauteur non-euclidienne ne se ferait sentir qu'à partir de  $k=10$  comme le lecteur pourra le vérifier. Reportons le parcours de l'intersection:

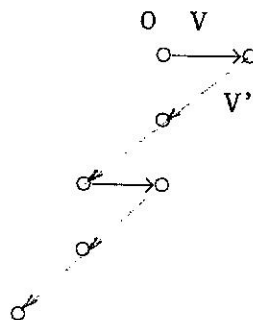


Fig. 1

ainsi que la position des points de coordonnées entières dans l'intersection des deux bandes rationnelles; nous constatons l'égalité des deux.

$$2 \text{ Résolution des inéquations } \begin{cases} 0 \leq 13x-11y < 21 \\ 0 \leq 7x-4y < 10. \end{cases}$$

Le réseau des équations est  $\mathcal{R} \begin{pmatrix} 13-11 \\ 7 & -4 \end{pmatrix}$ ,  $\delta=25$ ,  $\varepsilon=14$ ; l'opérateur de retour est  $M = \frac{1}{25} \begin{pmatrix} -4 & 11 \\ -7 & 13 \end{pmatrix}$ . Les dimensions de la fenêtre sont ici  $k=21$  et  $h=10$ . Les vecteurs euclidiens  $U$  et  $U'$  engendrés à partir de  $(0,25)$  et  $(1,14)$  sont  $U'=(-1,11)$  et  $U=(-3,8)$ ; d'où, comme  $\kappa=-3<0$ , les vecteurs de parcours du réseau des équations  $A=U'-U=(2,3)$  et  $A'=-U=(1,-3)$ . Ceux du parcours des droites sont  $V=(1,1)$  et  $V'=(-4,-5)$ . Le rationnel pilote est  $\frac{\beta}{\gamma} = \frac{3}{11}$ . La suite des restes  $\left\{ \frac{3i}{11} \right\}$  tronquée par  $h=10$  est représentée dans un tableau analogue. Ici l'algorithme s'arrête dans la colonne  $i=8$ . Nous devons donc effectuer, à partir de 0 les déplacements indiqués dans les colonnes allant de 0 à 7.

i	0	1	2	3	4	5	6	7	8
r	0	3	6	9	1	4	7	2	5
p	2	4	6	9	11	13	18	20	22
$\Delta$	V	V	V	V'	V	V	V+V'	V	

Cette fois le parcours n'est plus celui d'une suite arithmétique ordinaire: dans la colonne  $i=6$  apparaît un déplacement "somme", caractéristique des points qu'il convient d'omettre dans les fenêtres non-euclidiennes. Le report du parcours de l'intersection est immédiat:

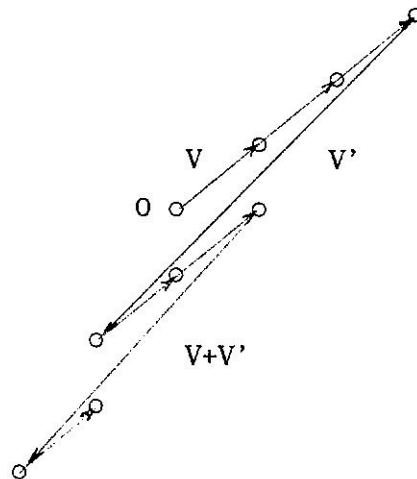


Fig. 2

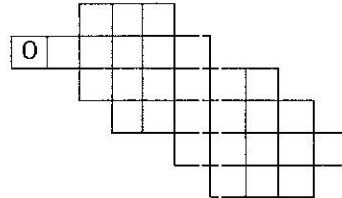
Nous constatons à nouveau le parfait accord avec les points entiers de l'intersection des bandes rationnelles associées.



donc les solutions de

$$\begin{cases} 0 \leq 5x + 7y < 29 \\ 0 \leq 2x - 3y < 29 \end{cases}$$

sont données par  $E' = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot E$ ,  $E$  étant considéré comme partie de  $\mathbb{Z}^2$ . On peut dessiner cet ensemble.



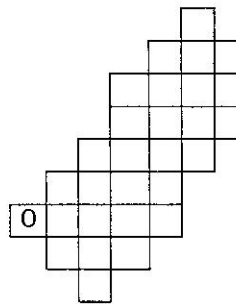
L'ensemble  $E'$

fig. 2

Si nous repartons de  $A$  et ôtons cette fois la deuxième colonne à la première le système devient

$$\begin{cases} 0 \leq 3x + 2y < 29 \\ 0 \leq 7x - 5y < 29 \end{cases}$$

et les solutions  $E''$  s'obtiennent par la transvection verticale de vecteur 1 sur  $E$ . La représentation graphique suit.



L'ensemble  $E''$

fig. 3

Ces deux exemples illustrent le résultat suivant.

proposition 1

a) *L'ajout à la colonne 1 de  $k$  fois la colonne 2 de  $A$  s'accompagne d'une transvection verticale de vecteur  $-k$ .*

b) L'ajout à la colonne 2 de  $k$  fois la colonne 1 de  $A$  s'accompagne d'une transvection horizontale de vecteur  $-k$ .

Si les deux composantes de la première ligne de  $A$  sont des entiers premiers entre eux, il sera toujours possible, par des manipulations sur ses colonnes, de la mettre sous la forme

$$\begin{pmatrix} 1 & 0 \\ c' & d' \end{pmatrix}$$

où  $c'$  et  $d'$  sont entiers. Les solutions du système associé sont par conséquent un segment de droite discrète, généralement épaisse. Il suffit de transformer ce segment par l'opérateur unimodulaire associé pour l'appliquer bijectivement sur l'ensemble des points d'intersection cherchés. Par ce biais nous montrons à nouveau que le problème de l'intersection a la complexité d'un tracé de droite discrète.

## V CONNEXITE DE L'INTERSECTION DE DEUX DROITES DISCRETES.

Dans cette partie nous abordons l'étude de la "topologie" de l'intersection de deux droites discrètes naïves  $\mathcal{D}(\frac{a}{b})$  et  $\mathcal{D}'(\frac{a'}{b'})$  passant par l'origine. Cette question contrôle directement la connexité des convexes et des polygones discrets; sa généralisation dans les dimensions supérieures est très importante.

A la fois pour des raisons de symétries et de simplicité nous supposons que les pentes vérifient les contraintes  $0 < \frac{a'}{b'} < \frac{a}{b} \leq 1$  et  $(a,b) = (a',b') = 1$  ce qui implique que l'épaisseur de  $\mathcal{D}(\frac{a}{b})$ , (resp.  $\mathcal{D}'(\frac{a'}{b'})$ ) est  $b$ , (resp.  $b'$ ). Le problème équivaut donc à la connexité de l'ensemble des solutions entières des inéquations

$$0 \leq a x - b y < b$$

$$0 \leq a' x - b' y < b',$$

la connexité étant prise au sens des 8 voisins. Le cas  $0 < \frac{a'}{b'} < 1 < \frac{a}{b}$  sera traité ultérieurement.

Supposons que le développement en fraction continue de la pente  $\frac{a}{b}$  soit donné:

$$\frac{a}{b} = [q_1, q_2, q_3, \dots, q_p]$$

### Théorème 1

L'intersection  $\mathcal{D}(\frac{a}{b}) \cap \mathcal{D}'(\frac{a'}{b'})$  est connexe si et seulement si on a l'une des inégalités

$$\frac{a'}{b'} < \begin{cases} \frac{1}{2q_1-1} & \text{si } q_1 \geq 1 \text{ et } q_2 = 0 \\ \frac{1}{2q_1+1} & \text{si } q_1 \geq 1 \text{ et } q_2 = 1 \\ \frac{1}{2q_1} & \text{si } q_1 \geq 2 \text{ et } q_2 \geq 2 \\ \frac{q_2}{q_2+2} & \text{si } q_1 = 1 \text{ et } q_2 \geq 2. \end{cases}$$

Cette condition, qui délimite un intervalle autour du rationnel  $\frac{a}{b}$  en dehors duquel il faut choisir la pente  $\frac{a'}{b'}$ , si l'on veut une intersection connexe, ne dépend que des deux premiers quotients partiels  $q_1$  et  $q_2$ . Les valeurs des diverses bornes peuvent être représentées facilement, comme l'indique le schéma suivant.

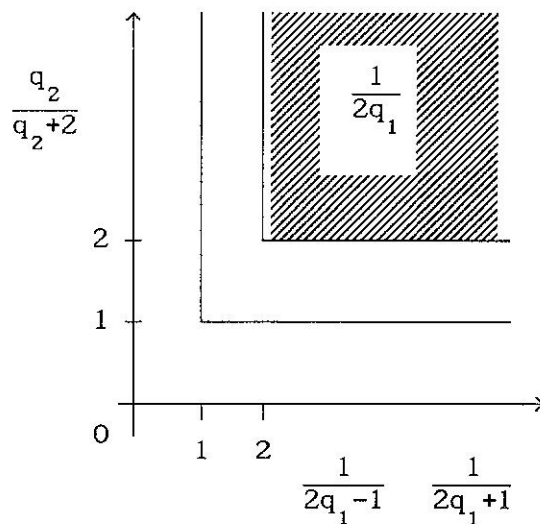


Fig. 1

démonstration

1° Cas  $q_2=0, q_1 \geq 2$ .

Si  $x=2q_1-2$ , alors on a  $\left[ \frac{x}{q_1} \right] = 1$ ,  $\left[ \frac{x}{2q_1-1} \right] = 0$ ; par contre si  $x=2q_1-1$  on a les égalités  $\left[ \frac{x}{q_1} \right] = \left[ \frac{x}{2q_1-1} \right] = 1$ . Ceci montre que l'intersection des droites discrètes  $\mathcal{D}\left(\frac{1}{q_1}\right)$  et  $\mathcal{D}\left(\frac{1}{2q_1-1}\right)$  n'est pas connexe. La situation est illustrée par la figure suivante:

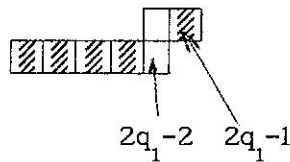


Fig. 2

On vérifie alors facilement que si  $\frac{a'}{b'} < \frac{1}{2q_1-1}$  alors  $\mathcal{D}(\frac{a}{b}) \cap \mathcal{D}(\frac{a'}{b'}) = \{(0,0), (1,0), \dots, (q_1-1,0)\}$ , qui est connexe. Par contre si  $\frac{a}{b} = \frac{1}{q_1} > \frac{a'}{b'} \geq \frac{1}{2q_1-1}$  alors cette intersection n'est pas connexe.

La preuve est analogue pour  $q_2=0$  et  $q_1=1$  ainsi que pour  $q_2=1$  et  $q_1 \geq 1$ ; en fait on sait que l'on a toujours l'égalité  $[q_1,1]=[q_1+1]$ .

2° Cas  $q_1 \geq 2, q_2 \geq 2$ .

En considérant les deux abscisses consécutives  $2q_1-1$  et  $2q_2$  nous constatons comme ci-dessus que  $\mathcal{D}(\frac{a}{b}) \cap \mathcal{D}(\frac{1}{2q_1})$  n'est pas connexe de même que pour  $\mathcal{D}(\frac{a}{b}) \cap \mathcal{D}(\frac{a'}{b'})$  lorsque  $\frac{a}{b} > \frac{a'}{b'} \geq \frac{1}{2q_1}$ . Par contre  $\forall \frac{a'}{b'} < \frac{1}{2q_1}$  l'intersection correspondante  $\mathcal{D}(\frac{a}{b}) \cap \mathcal{D}(\frac{a'}{b'})$  est connexe.

3° Cas  $q_1=1, q_2 \geq 2$ .

Le cas  $q_2=1$  est trivial. Nous subdivisons ce cas en distinguant selon la parité du quotient partiel  $q_2$ .

Supposons  $q_2$  impair.

Considérons les points  $M = (\frac{q_2+1}{2}, \frac{q_2-1}{2})$  et  $N = (q_2+2, q_2)$  de  $\mathbb{Z}^2$ . Nous pouvons faire les remarques suivantes:

○ Ces deux points ne sont pas consécutifs (en effet  $q_2 + 2 - \frac{q_2+1}{2} = \frac{q_2+1}{2} + 1$ ).

○ Ces deux points appartiennent à la droite naïve  $\mathcal{D}(\frac{a}{b})$ .

○ Pour tout  $i \in [0, \frac{q_2+1}{2}]$  le point  $(i, i-1)$  est également sur  $\mathcal{D}(\frac{a}{b})$ .

○ Pour tout  $i \in [0, \frac{q_2+1}{2}]$  les pentes  $\frac{i-1}{i}$  sont croissantes.

○ Le point  $M' = (\frac{q_2+1}{2} + 1, \frac{q_2+1}{2}) = (\frac{q_2+3}{2}, \frac{q_2+1}{2})$  est également situé sur  $\mathcal{D}(\frac{a}{b})$

immédiatement après M.

○ Mais pour  $i = \frac{q_2+1}{2} + 1$  on vérifie que l'on a les relations

$$\frac{q_2}{q_2+2} < \frac{\frac{q_2+1}{2}}{\frac{q_2+1}{2} + 1} = \frac{q_2+1}{q_2+3}$$

Cette fois la situation est décrite par la figure suivante.

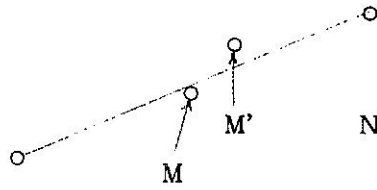


Fig. 3

Il s'ensuit que l'intersection  $\mathcal{D}(\frac{a}{b}) \cap \mathcal{D}(\frac{q_2}{q_2+2})$  n'est pas connexe mais que,

$\forall \frac{a'}{b'} < \frac{q_2}{q_2+2}$  l'intersection  $\mathcal{D}(\frac{a}{b}) \cap \mathcal{D}(\frac{a'}{b'})$  est connexe.

De plus pour tout rationnel  $\frac{a'}{b'}$ , vérifiant

$$\frac{q_2}{q_2+2} \leq \frac{a'}{b'} < \frac{a}{b}$$

l'intersection  $\mathcal{D}(\frac{a}{b}) \cap \mathcal{D}(\frac{a'}{b'})$  est non connexe. Il suffit de considérer la ligne polygonale réelle formée des paliers et des sauts verticaux sur une période de  $\mathcal{D}(\frac{a}{b})$ . La droite réelle de pente  $\frac{a'}{b'}$  la rencontre obligatoirement sur l'un de ses sauts verticaux. Il en résulte que l'intersection ne peut pas être connexe.

Le cas  $q_2$  pair est analogue.

ROTATIONS DISCRETES ET APPLICATIONS

## INTRODUCTION

C'est en essayant d'illustrer sur écran le phénomène de Moiré, créé par superposition deux grilles identiques légèrement décalées, que nous avons constaté les difficultés à faire **tourner** correctement une image discrète d'un angle quelconque. Il est clair qu'il n'existe pas, au sens strict, de rotation discrète d'angle quelconque dans  $\mathbb{Z}^2$ . Ce constat a suscité, non seulement en Infographie mais dans d'autres domaines où la Géométrie Discrète est présente: Architectures Parallèles, Automates Cellulaires,... le désir d'en obtenir de bonnes approximations discrètes et de caractériser objectivement leurs propriétés. Plusieurs approches ont été proposées, non seulement pour la rotation discrète, mais aussi pour les homothéties, homographies et autres transformations classiques (cf [2], [8], [58] ).

C'est dans le but de traiter ces conflits entre les notions continues et discrètes que nous proposons la Géométrie Discrète et le Calcul en Nombres Entiers. La question de la rotation discrète peut en principe être attaquée par ces deux outils.

Après une analyse des difficultés présentées par les transformations géométriques discrètes, nous aborderons dans cette partie deux algorithmes de rotation discrète: la **rotation compensée**, qui n'utilise du Calcul en Nombres Entiers que la présentation déjà faite au début de ce travail, et la **rotation-permutation** qui repose sur la Géométrie Discrète. Le premier algorithme est simple, rapide et assez général mais il présente encore des défauts. Bien que ceux-ci soient analysables par nos méthodes, ce qui permettrait de l'améliorer, il est moins intéressant que celui que fournit la Géométrie Discrète; ce dernier est très proche de l'optimalité.

Les autres transformations classiques (homothéties, homographies...) peuvent être abordées de façon analogue.

Nous présenterons ensuite le phénomène de Moiré dont la simulation sur ordinateur à servi, comme nous l'avons déjà dit, de fil conducteur.

## I LES APPROCHES EXISTANTES DE LA ROTATION DISCRETE.

1 La rotation réelle tronquée.

L'approche évidente mentionnée dans la littérature préconise l'usage de matrices de rotation et d'approximations pour aboutir aux coordonnées entières des pixels. Ces troncatures introduisent de nombreux défauts: deux pixels

peuvent avoir le même transformé et un point de l'image finale peut ne pas être atteint. C'est d'autant plus décevant que les calculs nécessaires sont longs.

## 2 La rotation par droites discrètes.

Le principe d'une rotation discrète bijective est simple: balayer  $\mathbb{Z}^2$  de deux manières: avec les droites  $y=cste$  puis avec les droites naïves  $y=\lfloor \frac{ai}{b} \rfloor + cste$  et appliquer les droites de la première famille sur celles de la deuxième de sorte que l'axe des  $y$  soit transformé en une droite perpendiculaire à la direction des droites naïves. La figure suivante illustre ce procédé.

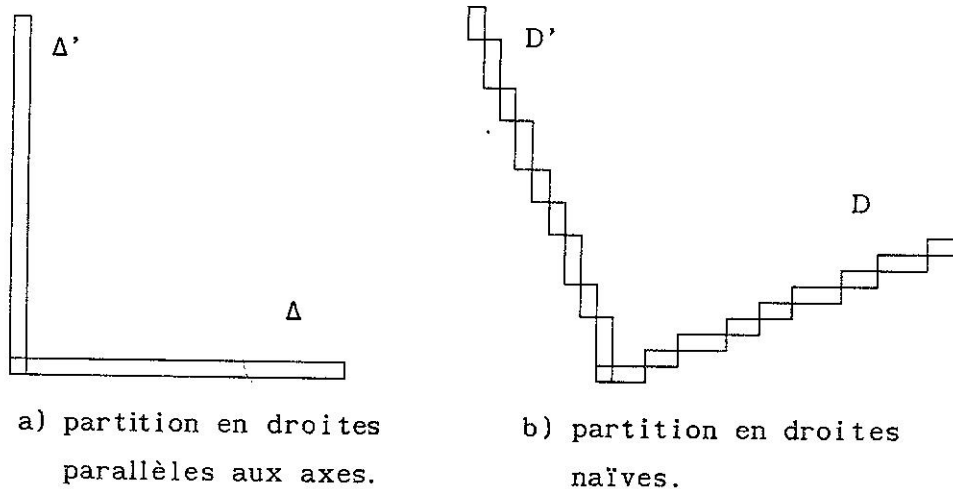


fig. 1

En a) figure la partition de  $\mathbb{Z}^2$  par les droites parallèles à l'axe des  $x$  désigné par  $\Delta$ ; en b) une partition de  $\mathbb{Z}^2$  par des droites parallèles à une direction  $D$  donnée formant un angle quelconque avec l'axe des  $x$ . Sur cette deuxième figure  $D'$  représente la droite orthogonale à la direction  $D$  passant par l'origine.

Cette idée n'est pas originale, elle est à la base de plusieurs tentatives. Mais le tracé naïf (ou celui de Bresenham) utilisé ici ne convient pas. Une implémentation de cet algorithme montre que l'image tournée est compressée dans la direction  $\Delta'$ : la transformation n'est pas **isométrique**. Ce défaut vient de la **non préservation des distances** du tracé naïf.

Plus précisément la longueur euclidienne d'un segment faisant un angle  $\alpha$  avec l'axe des abscisses croît en  $\frac{1}{\cos\alpha}$  jusqu'à  $\alpha = \frac{\pi}{4}$  puis décroît selon la même loi entre  $\frac{\pi}{4}$  et  $\frac{\pi}{2}$ , le phénomène se reproduisant dans les autres quadrants. Or, si  $0 \leq \alpha \leq \frac{\pi}{4}$ , le nombre de pixels de ces segments est **constant**; ce nombre ne

donne donc pas leur **longueur euclidienne**. Les difficultés de l'approche précédente de la rotation discrète viennent de là.

Si par exemple nous convenons qu'un segment horizontal de 19 pixels a une longueur euclidienne de 19 unités, le tracé naïf du segment de pente  $\frac{7}{19}$  apparaissant sur la figure suivante:

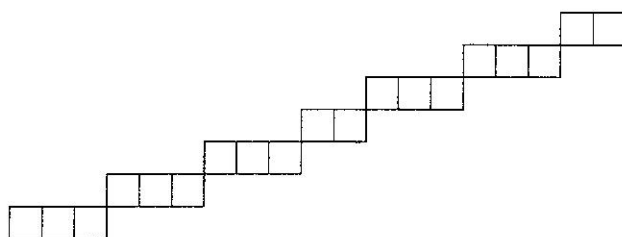
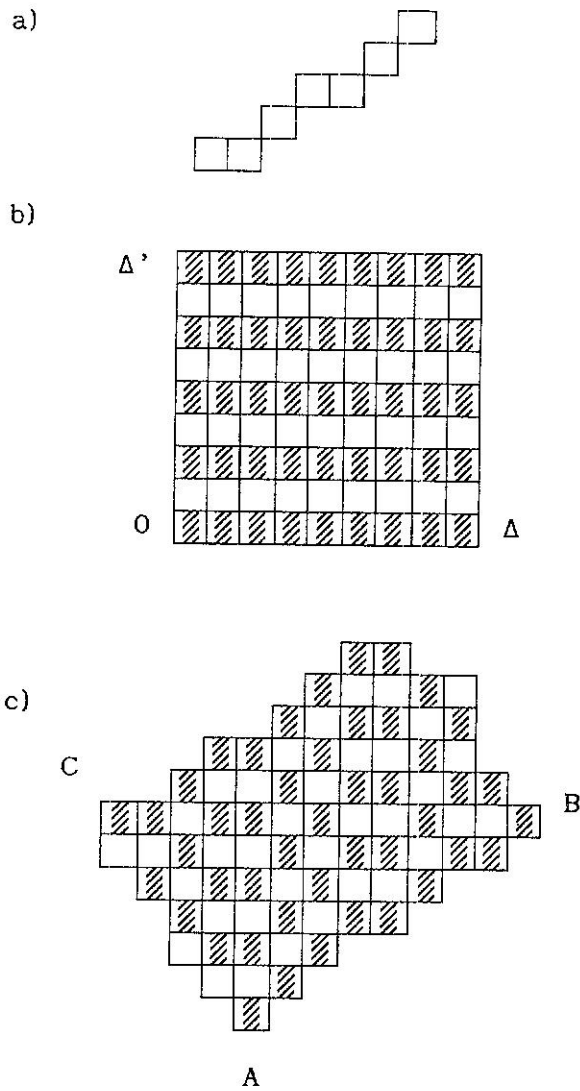


fig.2

aura une longueur euclidienne de  $\sqrt{410}$ , supérieure à 20.

Si nous revenons à l'idée évidente résumée dans la figure 1, à tout partage de  $\mathbb{Z}^2$  en droites parallèles est associé une rotation discrète appliquant bijectivement  $\Delta$  sur  $D$  puis les droites adjacentes à  $\Delta$  sur les adjacentes à  $D$  tout en envoyant  $\Delta'$  sur  $D'$ . Ce faisant la bijectivité globale est assurée mais pas nécessairement l'isométrie. La transformation  $R$  induite sera en général une homothétie discrète.

Il suffit de regarder un exemple. Partons d'un balayage de  $\mathbb{Z}^2$  en droites discrètes naïves introduites dans la première section. Ceci est facile à réaliser, il suffit de juxtaposer des droites identiques. La figure suivante illustre un tel balayage de  $\mathbb{Z}^2$  lorsque la pente de  $D$  est  $5/7$ ; a) représente le motif de la droite naïve de pente  $5/7$ , qu'il suffit de prolonger par périodicité pour obtenir une droite complète b) représente la partition initiale et c) la partition image. Nous constatons immédiatement le défaut d'isométrie.



AB direction D, AC direction D'

fig. 3

Concluons cette analyse en constatant que l'utilisation des matrices réelles et des troncatures l'algorithme conduit à des pertes d'information difficilement repérables; celle des balayages de  $\mathbb{Z}^2$  par des droites naïves (ou de Bresenham) l'algorithme préserve l'information mais déforme l'image. Bien que la conservation rigoureuse de l'isométrie ne soit pas possible, il est possible d'améliorer celle des droites naïves. Nous essaierons plus loin d'imposer aussi la bijectivité de la transformation.

## II LA ROTATION COMPENSEE.

Ce premier algorithme (résultat d'un travail commun avec A. Troesch), de rotation discrète utilise un tracé de droite discrète préservant les distances. Ce tracé, issu des méthodes de la dernière partie (le Calcul en

Nombres Entiers), diffère de ceux que nous avons introduit dans la première section consacrée aux droites discrètes. Il permet de corriger le défaut, évoqué ci-dessus, de non-isométrie des droites naïves.

### 1 Les droites compensées et l'invariance par rotation.

Pour sortir de cette situation nous introduisons un nouvel algorithme de tracé de droite préservant l'isométrie. Ce but est atteint par un parcours qui provoque des **attentes** ponctuelles isolées. Il est issu de l'intégration en nombres entiers du système différentiel

$$\begin{cases} X' = b \\ Y' = a \end{cases}$$

avec intervention d'un paramètre entier supplémentaire  $\omega$ .

Les entiers  $a$  et  $b$  sont les composantes d'un vecteur  $OM$  de  $\mathbb{Z}^2$ . Définissons quatre suites arithmétiques comme suit:

$$Rx = \left\{ \frac{bi+\epsilon}{\omega} \right\}, \quad x = \left[ \frac{bi+\epsilon}{\omega} \right],$$

$$Ry = \left\{ \frac{ai+\eta}{\omega} \right\}, \quad y = \left[ \frac{ai+\eta}{\omega} \right]$$

où  $\left\{ \frac{a}{b} \right\}$  désigne toujours le reste de la division entière de  $a$  par  $b$  et où  $\epsilon$  et  $\eta$  sont deux paramètres entiers permettant d'ajuster les initialisations des suites de restes  $Rx$  et  $Ry$ . Autrement dit les droites compensées sont définies par un double paramétrage en droites discrètes. Si nous prenons  $\epsilon = \eta = \left[ \frac{\omega}{2} \right]$  nous forçons l'apparition d'arrondis plutôt que de troncatures dans les calculs i.e. les deux composantes sont de type Bresenham.

La version incrémentale de cet algorithme se présente comme suit:

a) initialisations:

$$x_0 = 0, Rx_0 = \varepsilon, y_0 = 0, Ry_0 = \eta$$

b) récurrences:

$$Rx_{i+1} = (Rx_i + b) \bmod \omega \quad (1)$$

$$x_{i+1} = x_i + (Rx_i + b) \operatorname{div} \omega$$

$$Ry_{i+1} = (Ry_i + a) \bmod \omega$$

$$y_{i+1} = y_i + (Ry_i + a) \operatorname{div} \omega$$

En prenant pour  $x_0$  et  $y_0$  deux valeurs entières quelconques nous obtenons un tracé de segment d'origine quelconque. Nous appellerons **droite compensée** le tracé résultant de cet algorithme. Le coefficient de compensation  $\omega$  sera également appelé l'unité ou la vitesse.

La première propriété de ce tracé, sa pseudo-périodicité, résulte de la proposition évidente suivante.

#### Proposition 1

*Les suites  $Rx_i$  et  $Ry_i$  sont périodiques de période  $\omega$ .*

La pseudo-périodicité est l'assertion suivante:

$$\forall i \quad y_{i+\omega+1} - y_{i+\omega} = y_{i+1} - y_i$$

qui signifie que les incréments de  $y_i$  (ou dérivée discrète) forment une suite périodique.

Par construction une droite compensée contient:

- des points stationnaires,
- des sauts 8-connexes,
- des sauts 4-connexes.

Il est facile, sur des exemples, de vérifier l'existence de ces diverses situations.

Le paramètre  $\omega$  apporte alors une certaine **élasticité** aux segments qu'il engendre, ce qui les rend intéressants pour les transformations géométriques. Dans le cas de la rotation l'isométrie est contrôlée par la condition

$$a^2 + b^2 = \omega^2 \quad (2)$$

Ceci se traduit par le théorème suivant dont la vérification est immédiate.

### Théorème 1

Supposons que  $a, b, \omega$  satisfassent à (2) et que les suites  $x_i, Rx_i, y_i$  et  $Ry_i$  soient initialisées comme en (1) avec  $0 \leq \varepsilon < \omega$  et  $0 \leq \eta < \omega$ , alors pour  $i \leq \omega$  la partie entière de la longueur euclidienne du segment joignant l'origine de  $\mathbb{Z}^2$  au point  $(x_i, y_i)$  est égale à  $i$  ou à  $i+1$ .

Autrement dit la mesure euclidienne d'un segment est comptée par le nombre d'itérations de l'algorithme (1) avec au plus une erreur d'une unité. De plus si l'équation (2) n'a pas de solution il est possible de prendre une valeur de  $\omega$  égale à

$$\omega = \left[ \sqrt{a^2 + b^2} \right]$$

ou à

$$1 + \left[ \sqrt{a^2 + b^2} \right]$$

ou bien de prendre parmi les deux entiers précédents celui qui est le plus proche de  $\sqrt{a^2 + b^2}$ , chacun de ces choix conduit à un résultat identique à celui du théorème.

Si nous reprenons notre exemple du §1 d'un segment de pente  $\frac{7}{19}$  nous constatons que l'algorithme nécessite  $\omega=20$  itérations pour tracer le segment sur une période et provoque une attente en  $i=0$  si  $\varepsilon=0$  et  $\eta=0$  et une attente en  $i=10$  si les initialisations sont données par  $\varepsilon=\eta=\left[\frac{\omega}{2}\right]$ . Les initialisations  $\varepsilon$  et  $\eta$  permettent donc de contrôler en partie les positions des points d'attente à l'intérieur de la période.

Signalons que la juxtaposition des droites compensées n'est pas parfaite. Si nous prenons deux points contigus  $O$  et  $O'$  (mêmes abscisses et ordonnées consécutives) alors les deux segments compensés  $OM$  et  $O'M'$  issus de  $O$  et  $O'$ , de même pente et même longueur, ne seront, en général, ni disjoints ni parfaitement accolés : il peut exister des pixels n'appartenant ni à  $OM$  ni à  $O'M'$  entourés par des points de ces derniers et des pixels communs à  $OM$  et  $O'M'$ .

## 2 Le balayage par les droites compensées et la rotation discrète.

Nous utilisons comme dans [58] un balayage horizontal de l'image finale et un balayage d'angle  $\alpha$  de l'image initiale. Mais nous utiliserons, pour ce dernier des droites compensées. L'écran final est donc divisé en lignes horizontales et nous recherchons les points qui leur correspondent sur l'image initiale pour pouvoir reporter les attributs de couleur. L'analyse de l'image

finale nécessite en fait deux parcours de droites, celui déjà mentionné étant le balayage rapide; un deuxième, le balayage lent consiste à décrire les points de départ des lignes du balayage rapide; ces points sont situés sur une droite verticale, la droite d'appui. Dans l'image initiale la droite d'appui est une droite de pente  $\alpha'$  orthogonale à  $\alpha$ . Les deux balayages rapides peuvent être considérés comme des solutions de deux champs de vecteurs constants de même module, analogues à des vecteurs vitesse, ce qui explique la terminologie précédente. Pour trouver les points correspondants sur les deux images il suffit donc d'intégrer ces deux champs simultanément ce qui revient à utiliser l'algorithme de tracé (1).

Les paramètres constitués par les conditions initiales des tracés rapides sont encore indéterminés jusque là. D'un point de vue théorique nous pouvons supposer chaque pixel constitué de  $\omega^2$  micropixels. A chaque pas, l'algorithme de tracé d'une droite compensée détermine, en plus du pixel de la droite proprement dit, et à l'intérieur de celui-ci, un micropixel distingué. Si dans chaque pixel nous choisissons un microrepère d'origine le coin inférieur droit, d'axes les directions principales de l'écran et d'unité le micropixel, les coordonnées du micropixel distingué dans le pixel sont les restes  $R_x$  et  $R_y$ . Ces micropixels sont tous parfaitement alignés sur la droite réelle que la droite compensée est supposée représenter. Il est donc naturel d'initialiser les restes des droites de balayage par les coordonnées des micropixels distingués de la droite d'appui. Ce choix conduit en général à une répartition assez "homogène" des trois types de défauts: les trous, les points stationnaires et les recouvrements. Nous montrerons ci-dessous comment nous parvenons à localiser ces défauts.

Donnons quelques détails sur l'implantation de cet algorithme de balayage. Il applique le carré de sommets  $S_1=(X_{Linit}, Y_{Linit})$ ,  $S_2=S_1+X_{max}(\cos\alpha, \sin\alpha)$ ,  $S_3=S_2+X_{max}(-\sin\alpha, \cos\alpha)$ ,  $S_4=S_3+X_{max}(-\cos\alpha, -\sin\alpha)$  où  $\cos\alpha = \frac{a}{\omega}$  et  $a^2+b^2=\omega^2$  sur le carré  $[X_{finit}, X_{finit}+X_{max}] \times [Y_{finit}, Y_{finit}+X_{max}]$ .

Soient  $v_f=(\omega, 0)$  et  $v_i=(a, b)$  les deux vecteurs vitesse de balayage respectifs de l'image finale et de l'image initiale,  $\omega^2$  étant voisin de  $a^2+b^2$  et du même ordre de grandeur que la plus grande dimension en pixels de l'image. Les vecteurs orthogonaux correspondants sont alors  $w_f=(0, -\omega)$  et  $w_i=(b, -a)$ . Soient  $X_i$  et  $Y_i$  les coordonnées sur l'écran initial,  $X_f$  et  $Y_f$  les coordonnées sur l'image finale  $RX_i, RY_i, RX_f, RY_f$  les restes correspondants (ces notations diffèrent de celles du § précédent). Nous donnons ci-dessous l'algorithme complet de rotation discrète pour une image carrée de  $X_{max}$  pixels

de côté.

```

XL:=XLinit;
YL:=YLinit;
RXL:=0; RYL:=0;
Yf:=Yfinit;
Tant que Yf < Xmax
faire
debut
{ balayage lent }
  RXL:=RXL+b;
  RYL:=RYL-a;
  XL:=XL+RXL div ω;
  YL:=YL+RYL div ω;
  RXL:=RXL mod ω;
  RYL:=RYL mod ω;
  { XL, YL: coordonnées
  des débuts de lignes
  de balayage }

```

```

Xi=XL;
Yi=YL;
Yf:=Yf+1; Xf:=Xfinit;
RXi=RXL;
RYi=RYL;
tant que Xf < Xmax
faire
  début
  { balayage rapide }
    RXi:=RXi+a;
    RYi:=RYi+b;
    Xi:=Xi+RXi div ω;
    Yi:=Yi+RYi div ω;
    RXi:=RXi mod ω;
    RYi:=RYi mod ω;
    Xf:=Xf+1;
  fin;
fin;

```

Dans cet algorithme nous supposons que les opérations div et mod ont les propriétés suivantes:

$$R \bmod \omega \geq 0$$

$$R = (R \operatorname{div} \omega) * \omega + R \bmod \omega$$

quel que soit le signe de R, ω étant toujours supposé positif. Signalons qu'une implémentation Pascal de l'algorithme précédent permet de faire tourner d'un angle quelconque une image bit-map 150x150 en 5s environ sur un AT 8 Mhz.

### 3 Les défauts de la rotation compensée.

Pour simplifier un peu ce paragraphe nous supposons que la droite discrète compensée de pente  $\frac{a}{b}$  utilisée est paramétrée par

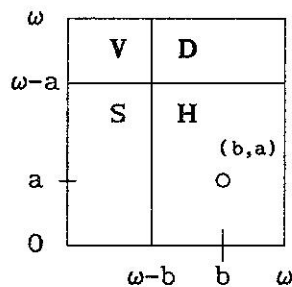
$$M(t) = \begin{cases} \left\lceil \frac{bt}{\omega} \right\rceil \\ \left\lceil \frac{at}{\omega} \right\rceil \end{cases} \quad \text{où } t \in \mathbb{Z}.$$

En utilisant les propriétés des droites discrètes via les suites de restes

$\left\{\frac{at}{\omega}\right\}$  et  $\left\{\frac{bt}{\omega}\right\}$  nous voyons que le point  $M(t)$  est suivi d'un déplacement:

- horizontal ssi  $\left(\left\{\frac{bt}{\omega}\right\}, \left\{\frac{at}{\omega}\right\}\right) \in [\omega-b, \omega[ \times [0, \omega-a[$
- diagonal ssi  $\left(\left\{\frac{bt}{\omega}\right\}, \left\{\frac{at}{\omega}\right\}\right) \in [\omega-b, \omega[ \times [\omega-a, \omega[$
- vertical ssi  $\left(\left\{\frac{bt}{\omega}\right\}, \left\{\frac{at}{\omega}\right\}\right) \in [0, \omega-b[ \times [\omega-a, \omega[$
- stationnaire ssi  $\left(\left\{\frac{bt}{\omega}\right\}, \left\{\frac{at}{\omega}\right\}\right) \in [0, \omega-b[ \times [0, \omega-a[$ .

Il est commode de représenter ces quatre cas sur un schéma comme ci-dessous:



Il suffit donc d'étudier la suite  $t.(b, a) \bmod \omega$  avec  $t=0, 1, \dots, \omega-1$  pour connaître la structure de la période de la droite compensée. Il est clair que si  $(a, \omega) = (b, \omega) = 1$  la suite  $\left(\left\{\frac{bt}{\omega}\right\}, \left\{\frac{at}{\omega}\right\}\right)_{t \in [0, \omega[}$  est encore le graphe d'une **permutation**. Cette permutation s'écrit aussi  $(t, \left\{\frac{\varepsilon t}{\omega}\right\})$  où  $\varepsilon b \equiv a \pmod{\omega}$  c'est à dire  $\varepsilon \equiv ab^{-1} \pmod{\omega}$ . Nous obtenons

### Théorème 2

*La période de la droite compensée associée au triple pythagoricien  $(a, b, \omega)$  possède  $\omega-b$  points particuliers qui sont des points stationnaires ou des sauts 4-connexes.*

Ceci précise la propriété d'isométrie donnée dans le théorème 1. De plus les propriétés de structure des suites arithmétiques dégagées dans les premières sections de ce travail permettraient de localiser plus finement la position de chacun des types de déplacement à l'intérieur de la période.

Plusieurs cas particuliers intéressants apparaissent:

- 1 Les triples  $a, b, b+1$ .

La classification précédente montre que dans ce cas la période contient

- 1 point stationnaire,
- 0 saut 4-connexe.

Par conséquent les droites compensées associées à ces triples se juxtaposent parfaitement et la rotation associée ne contient qu'un type de défaut: une perte d'information due à une répétition de pixel au taux de  $\frac{1}{b+1}$ .

2 Les triples  $a, b, b+2$ .

Les résultats sur les suites arithmétiques montrent que la période de ces droites compensées ont:

- 1 point stationnaire,
- 1 saut 4-connexe au milieu du segment.

Mais les droites compensées ainsi définies ne sont pas des droites discrètes au sens de la première section; par conséquent elles ne peuvent pas, en général, le plan  $\mathbb{Z}^2$ . Les rotations associées ont encore de bonnes propriétés métriques mais contiennent deux pertes d'information par période.

La rotation compensée a surtout l'avantage d'être généralisable simplement à toute transformation continue plane définie par un système différentiel, cf. §IV suivant.

### III LA ROTATION-PERMUTATION.

Soit à nouveau un triple pythagoricien  $(a,b,\omega)$ . Nous allons montrer que la transformation qui applique le point entier  $(x,y)$  sur le point entier de coordonnées:

$$\begin{array}{l}
 x + \left[ \frac{(b-\omega)y}{a} \right] + \left[ \frac{(b-\omega) \left( y + \left[ \frac{a(x + \left[ \frac{(b-\omega)y}{a} \right])}{\omega} \right] \right)}{a} \right] \\
 y + \left[ \frac{a(x + \left[ \frac{(b-\omega)y}{a} \right])}{\omega} \right]
 \end{array}$$

est une bonne approximation discrète de la rotation d'angle  $\text{Arctg}(\frac{a}{b})$ . De plus cette transformation est une **permutation** de  $\mathbb{Z}^2$ .

## 1 Une identité matricielle.

Cette formule résulte de la discrétisation de la décomposition d'une matrice de rotation en produit de trois transvections:

$$\begin{pmatrix} \frac{b}{\omega} & -\frac{a}{\omega} \\ \frac{a}{\omega} & \frac{b}{\omega} \end{pmatrix} = \begin{pmatrix} 1 & \frac{b-\omega}{a} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \frac{a}{\omega} & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{b-\omega}{a} \\ 0 & 1 \end{pmatrix}.$$

Ce qui peut être traduit symboliquement, en commettant un abus de langage, par la notation suivante:

$$\begin{pmatrix} 1 & [\frac{b-\omega}{a}] \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ [\frac{a}{\omega}] & 1 \end{pmatrix} \begin{pmatrix} 1 & [\frac{b-\omega}{a}] \\ 0 & 1 \end{pmatrix}$$

donnant la composition de trois transformations de  $\mathbb{Z}^2$ . La première, par exemple, est en fait l'application définie par

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x + [\frac{(b-\omega)y}{a}] \\ y \end{pmatrix}.$$

Le tout conduisant à la formule de rotation. Vérifions les propriétés annoncées.

## 2 Les quasi-transvections.

### Définition

Pour tout rationnel  $\frac{a}{\omega}$  nous désignons par **quasi-transvection horizontale** de vecteur  $\frac{a}{\omega}$  la transformation de  $\mathbb{Z}^2$  induite par

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x + [\frac{ay}{\omega}] \\ y \end{pmatrix}$$

que l'on notera "matriciellement" par

$$\begin{pmatrix} 1 & [\frac{a?}{\omega}] \\ 0 & 1 \end{pmatrix}.$$

Les quasi-transvections verticales sont définies de manière analogue.

Ces quasi-transvections sont des **bijections** de  $\mathbb{Z}^2$ , la réciproque de

$$\begin{pmatrix} 1 & [\frac{a?}{\omega}] \\ 0 & 1 \end{pmatrix}$$

étant

$$\begin{pmatrix} 1 & -[\frac{a?}{\omega}] \\ 0 & 1 \end{pmatrix}.$$

Les propriétés "globales" de ces transformations s'expriment bien à l'aide des droites discrètes et de généralisations assez proches de celles-ci qui seront étudiées ailleurs.

Théorème 1

La quasi transvection verticale  $\begin{pmatrix} 1 & 0 \\ \left[ \frac{a?}{\omega} \right] & 1 \end{pmatrix}$  où  $0 \leq a < \omega$ ,  $(a, \omega) = 1$ , transforme la droite discrète  $y = k$ ,  $k \in \mathbb{Z}$ , en la droite discrète  $k\omega \leq ax - \omega y < (k+1)\omega$ . (id. pour les quasi-transvections horizontales).

Théorème 2

Soit  $\varepsilon$  un entier tel que  $0 < \varepsilon < \inf(a, \omega - a)$ , alors la quasi-transvection horizontale  $\begin{pmatrix} 1 & -\left[ \frac{\varepsilon?}{a} \right] \\ 0 & 1 \end{pmatrix}$  transforme la droite discrète  $k\omega \leq ax - \omega y < (k+1)\omega$  en une structure proche de la droite discrète  $k\omega \leq ax - by < (k+1)\omega$  où on a posé  $\omega - \varepsilon = b$ .

3 Les propriétés métriques des droites pythagoriciennes.

Les propriétés métriques des droites discrètes sont remarquables lorsque leur vecteur normal  $(a, b)$  et leur épaisseur arithmétique  $\omega$  constituent un triple pythagoricien. Dans ce cas nous avons les inéquations:

$$0 \leq a \leq b \leq \omega \leq a+b$$

et la période de la droite discrète

$$k\omega \leq ax - by < (k+1)\omega$$

(i.e.  $x \in [0, b[)$  contient  $\omega = \sqrt{a^2 + b^2}$  points entiers, c'est à dire le même nombre que le segment  $[0, \omega [$ . Nous pouvons considérer que ce dernier a tourné d'un angle  $\text{Arctg}\left(\frac{a}{b}\right)$  sans perte d'information. Nous qualifions de **pythagoriciennes** ces droites discrètes.

Les droites pythagoriciennes précédentes préservent donc la longueur euclidienne des segments de la forme  $[0, k\omega]$   $k \in \mathbb{Z}$ .

Pour un segment  $[0, x]$  quelconque le vecteur différence entre les transformés du point  $(x, 0)$  par la rotation-permutation et la rotation réelle tronquée se met sous la forme:

$$\left( \begin{array}{c} \frac{1}{a} \left\{ \frac{(\omega-b) \lfloor \frac{ax}{\omega} \rfloor}{a} \right\} - \frac{(\omega-b)}{a\omega} \left\{ \frac{ax}{\omega} \right\} \\ 0 \end{array} \right)$$

dont la première composante se majore, dans tous les cas par 2 et, dans le cas particulier  $\omega-b=1$ , par 1. Ceci prouve le

### Théorème 3

a) Si  $\omega-b=1$  l'image du point  $(x,0)$  par la rotation-permutation à la même ordonnée que son transformé par la rotation réelle tronquée et son abscisse est soit identique soit augmentée de 1.

b) Si  $\omega-b > 1$  les ordonnées sont les mêmes et les abscisses diffèrent de 0, 1 ou 2.

Ceci montre l'optimalité de la rotation-permutation, au moins dans le cas a), qui restitue la bijectivité de la rotation discrète tout en ayant des propriétés métriques analogues à celles de la rotation réelle tronquée.

### Remarque.

L'algorithme précédent a encore un sens même si  $\omega$  ne vérifie pas l'égalité  $\omega = \sqrt{a^2+b^2}$ . Nous ne pouvons plus, dans ce cas, assurer les résultats précédents mais, expérimentalement, l'algorithme reste toutefois de bonne qualité si  $\omega$  est l'entier le plus voisin de  $\sqrt{a^2+b^2}$ . Nous dirons alors que nous avons une **rotation quasi-pythagoricienne**.

Par exemple avec  $a=5$ ,  $b=7$  et  $\omega=9$  le motif de la droite \*-connexe associée est le suivant:

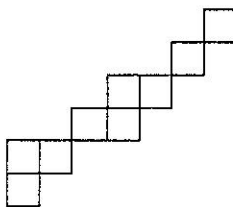


Fig. 4

Le pavage en droites \*-connexes associé est indiqué ci-dessous:

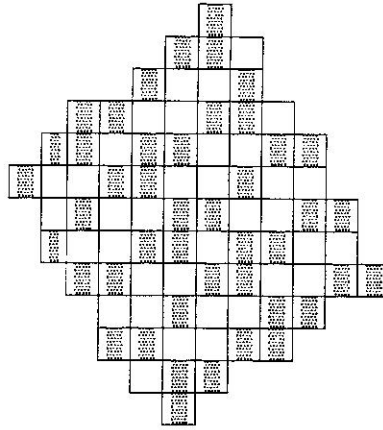


Fig. 5

le balayage quasi-pythagoricien

Sur la figure 5 nous avons représenté le transformé d'un carré de coté 9. L'amélioration de l'isométrie de la rotation discrète par rapport à celle de la fig. 3 est nette (les défauts qui apparaissent sont dus à l'imprimante).

#### IV AUTRES TRANSFORMATIONS.

De la même manière on peut traiter des transformations géométriques plus générales. Soit  $x_f = f(x_i, y_i)$ ,  $y_f = g(x_i, y_i)$ , une transformation du plan (nous supposerons  $f$  et  $g$  de classe  $C^1$ ). Si nous balayons toujours l'image finale horizontalement le balayage correspondant de l'image initiale sera obtenu par intégration du champ suivant :

$$V_1 = 1/J \frac{\partial g(x_i, y_i)}{\partial y_i}$$

$$V_2 = -1/J \frac{\partial g(x_i, y_i)}{\partial x_i}$$

où  $J$  est le Jacobien de la transformation au point  $(x_i, y_i)$ , les conditions initiales étant prises sur une courbe intégrale du champ

$$V_1 = -1/J \frac{\partial f(x_i, y_i)}{\partial y_i}$$

$$V_2 = 1/J \frac{\partial f(x_i, y_i)}{\partial x_i}$$

En particulier pour les transformations linéaires on obtient des champs constants. L'intégration en nombres entiers de ces champs conduit alors à la transformation cherchée. Ce procédé généralise donc l'algorithme de la rotation compensée.

## V LE MOIRÉ ARITHMÉTIQUE

### Introduction.

Le phénomène de Moiré a été observé depuis l'Antiquité; son occurrence la plus simple apparaît dans les **franges de Ronchi** (ou de Rayleigh). Elles sont obtenues par superposition de deux grilles de diffraction identiques. Le traitement mathématique de ce phénomène a été longtemps ouvert (cf. [76], [113]).

Depuis Rayleigh [92] proposant d'utiliser le moiré pour vérifier la qualité des grilles de Ronchi formées d'un très grand nombre de fins traits parallèles, le nombre d'applications du Moiré est vaste, du vernier aux appareils permettant d'observer le mélange de deux solutions. Il partage d'ailleurs plus que des analogies avec la théorie des phénomènes ondulatoires.

L'usage des écrans graphiques bit-map pose beaucoup de problèmes dont l'**aliassage** est un des plus délicats. Celui-ci ayant une parenté avec le Moiré, l'étude de ce dernier devrait amener à une meilleure compréhension de ces difficultés.

C'est ce qui nous conduit, dans ce chapitre, à discrétiser le Moiré et à étendre son rôle d'instrument de mesure à la Géométrie Discrète. Cette discrétisation s'opère en remplaçant les réseaux de diffraction par des **grilles de droites discrètes**.

### 1 Les lois générales du Moiré.

Le Moiré apparaît essentiellement lorsque deux grilles identiques, semblables aux courbes de niveaux du relief terrestre, sont superposées avec un petit décalage. Il se présente sous l'aspect de franges beaucoup plus larges que les traits constituant les grilles et dont les niveaux de gris ont un aspect très régulier. Le phénomène se produit également dans la superposition de deux grilles voisines, ce deuxième cas se ramenant au premier en considérant des décalages fonction de deux variables.

La détermination théorique des franges de Moiré comporte deux aspects:

- o l'équation des franges (en fait celle des courbes centrales ou axes des franges),
- o l'expression du niveau de gris de chacune d'elles.

Bien que la première partie soit connue, pour les cas les plus simples, depuis assez longtemps, la partie délicate de l'étude du Moiré consiste à évaluer les fonctions de densité des franges. Cette difficulté a été résolue assez récemment par J. Harthong ([56]) au moyen de l'ANS.

## 2 Les équations des franges.

Nous présentons ici les éléments les plus simples concernant la localisation des franges telle que nous pouvons la trouver dans les traités classiques déjà mentionnés et rappellerons le résultat essentiel de [56] concernant le calcul de leur densité. L'obtention des équations des centres des franges est assez simple; rappelons-en le principe.

Soient deux fonctions numériques différentiables  $\phi$  et  $\psi$  définies sur le plan  $\mathbb{R}^2$ , considérons les deux réseaux  $\mathbf{R}$  et  $\mathbf{S}$  formés des franges définies par les images réciproques par  $\phi$  et  $\psi$  des intervalles  $[2n, 2n+1[$  et  $[2n+1, 2n+2[$ , ( $n \in \mathbb{Z}$ ). Supposons ces franges alternativement colorées et noir et blanc.

Numérotons la frange  $\phi^{-1}([n, n+1[)$  du réseau  $\mathbf{R}$  par l'entier  $n$ ; opérons de même pour le réseau  $\mathbf{S}$ .

Nous observons maintenant une propriété fondamentale de ces franges: Supposons qu'une frange de Moiré contienne un domaine  $\delta(k, h)$  intersection de la frange  $k$  de  $\mathbf{R}$  et de la frange  $h$  de  $\mathbf{S}$ , alors l'un des éléments voisins de cette frange de Moiré est  $\delta(k+1, h-1)$  ou de  $\delta(k+1, h+1)$ . Autrement dit l'une des équations aux indices suivante

$$k-h = \text{Cste}$$

$$k+h = \text{Cste}$$

est vérifiée le long d'une frange de Moiré. Ce sont les équations aux indices d'une frange qui traduisent l'invariance de l'une des expressions  $k-h$  ou  $k+h$ .

Ces équations permettent de déterminer les équations des franges et de les numéroter elles aussi par leur invariant.

## 3 Le théorème de convolution de Harthong.

Observons un Moiré produit par la superposition de deux grilles, comme sur les figures suivantes. Nous observons que les franges n'ont pas un bord bien défini, la densité de gris semble varier presque continuellement lorsque nous nous déplaçons du milieu bien noir vers les bords où la densité de gris devient nulle. En regardant le bord de près nous constatons qu'il est formé de triangles noirs et blancs enchevêtrés. C'est cet enchevêtrement, dépendant des grilles, qui rend le traitement rigoureux de la densité de gris difficile. Nous partons d'un objet visiblement géométrique, la grille, présentant une structure à la fois discrète et continue et une densité de gris **rectangulaire** et nous obtenons des franges de Moiré où la répartition des densités de gris à visiblement changé.

-a) Si les grilles sont très voisines alors les franges sont très larges; il est facile d'expérimenter un peu et de constater ce fait.

-b) l'ANS permet de traiter rigoureusement des ordres de grandeur différents dans un même calcul; de plus des ensembles externes, aux propriétés

idéales, peuvent être introduits.

Il faut considérer une frange de Moiré de deux grilles infiniment voisines comme un ensemble externe, n'ayant pas de frontière, halo d'une courbe standard, axe de la frange. La densité de gris en tout point de ces franges s'évalue par un calcul, assez simple dans le cadre ANS, qui apporte, à cette question, une réponse à la fois simple et générale.

#### Théorème (Harthong)

*La densité des franges de Moiré est le produit de convolution des densités de chaque grille.*

Ceci explique les densités quasi-continues des franges même si celles grilles initiales sont discontinues (signaux rectangulaires).

#### 4 Le Moiré de droites continues.

Résumons ici les lois du Moiré de réseaux de Ronchi constitués de bandes alternativement noires et blanches; les densités sont donc des signaux carrés.

La superposition de deux réseaux identiques de bandes réelles de largeurs  $\ell$ , l'un étant tourné d'un angle  $\alpha$  par rapport à l'autre, donne des franges dont:

La **direction** est celle de la bissectrice extérieure des deux directions des réseaux.

L'**espacement** entre les franges est  $\frac{\ell}{\sin(\frac{\alpha}{2})}$ .

Le **niveau de gris moyen** est un signal triangulaire.

remarque: Si les deux grilles réelles superposées n'ont pas les mêmes largeurs il est facile de vérifier que les franges sont dirigées par la petite diagonale du parallélogramme obtenu en superposant une bande de chaque réseau.

#### 5 La discrétisation du Moiré.

Passons maintenant à la discrétisation du Moiré.

Supposons que nous superposions deux grilles identiques formées de bandes parallèles discrètes, alternativement noires et blanches, définies par:

$$k.\omega \leq ax+by < (k+1)\omega \quad k \in \mathbb{Z}$$

et

$$l.p \leq ac+dy < (l+1)p \quad l \in \mathbb{Z}$$

Discretisons la loi d'addition des couleurs comme suit:

blanc + blanc = blanc  
 blanc + noir = noir  
 noir + noir = noir.

Voici la figure de Moiré résultante successivement en pixels usuels et en pixels grossis 5x5.

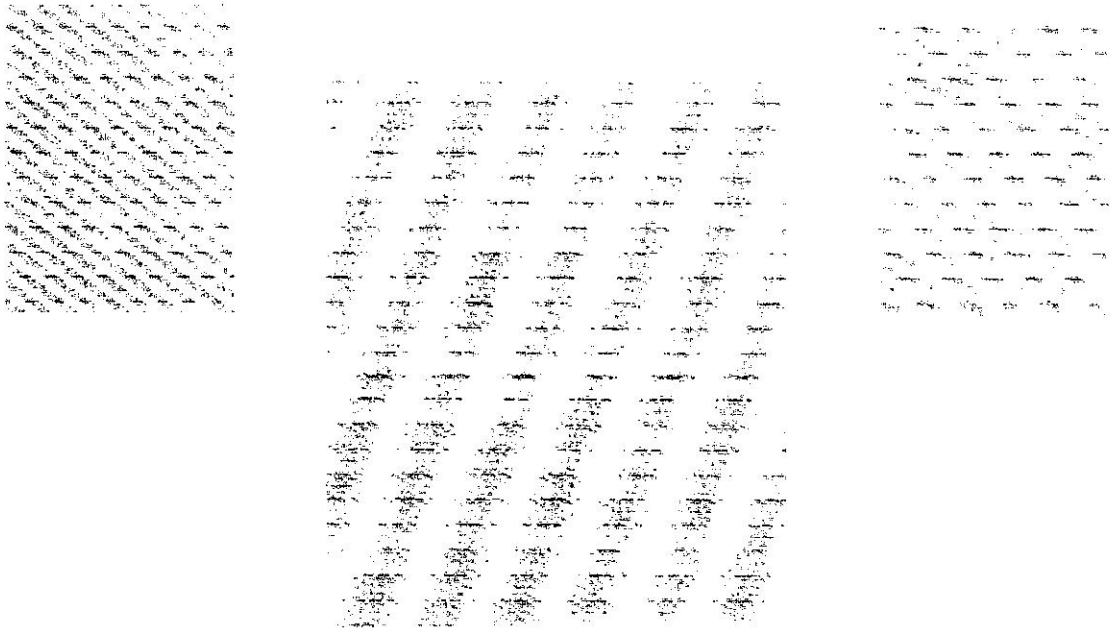


Fig. 1

Moiré des deux grilles d'équations:

$$23 k \leq 4x + 7y < 23 (k+1)$$

$$9 l \leq x + 3y < 9 (l+1)$$

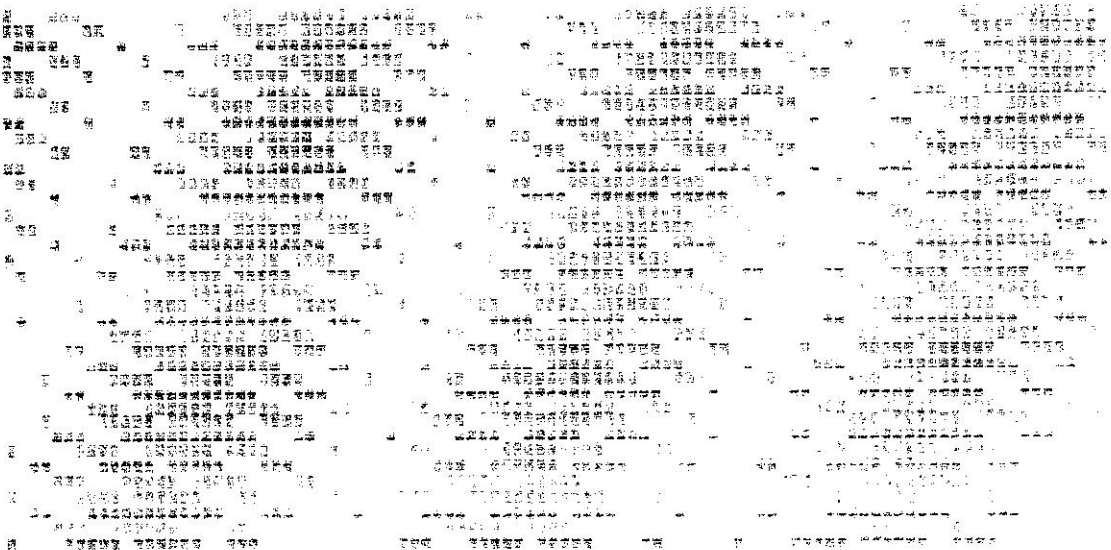


Fig. 2

Grossissement du Moiré des deux grilles d'équations:

$$23 k \leq 4x + 7y < 23(k+1)$$

$$9 l \leq x + 3y < 9(l+1)$$

## 6 Les lois du Moiré arithmétique.

Nous constatons que ce système de franges vérifie assez bien les lois du Moiré continu. Pouvons-nous expliquer arithmétiquement cet accord ?

Remarquons d'abord que les franges sont des réunions d'intersections de droites discrètes !

Il est facile de vérifier que les lois du Moiré arithmétique sont les suivantes:

La **direction** des franges est donnée par le vecteur  $(d\omega - b\rho, -c\omega + a\rho)$ .

La **distance** entre les franges est  $\frac{2|\omega\rho|}{\sqrt{(c\omega - a\rho)^2 + (d\omega - b\rho)^2}}$

La loi de **convolution** s'interprète en disant que:  
Le **nombre de pixels noirs** contenus dans la période d'une droite discrète parallèle à l'axe des franges varie à peu près linéairement comme le signal triangulaire  $1 - |x|$ .

## 7 Le problème des grilles isométriques.

Dans la simulation discrète du Moiré il est important de pouvoir disposer de grilles isométriques de directions quelconques. Ceci pose à nouveau le problème des propriétés métriques des droites discrètes.

La figure suivante illustre, en gros pixels, deux réseaux discrets, dont les largeurs (euclidiennes) ne sont pas voisines, et leur Moiré. On a aussi indiqué par un petit segment la direction des franges que l'on obtiendrait si les deux réseaux étaient isométriques. Nous avons également fait figurer l'espace interfrange.

La réalisation de grilles discrètes de pentes distinctes et de même largeur pose un problème de contrôle global de la métrique en Géométrie Discrète analogue à celui de la rotation discrète. Il nécessite un traitement convenable.

La loi de direction des franges du Moiré discret va nous servir d'instrument pour **mesurer** l'isométrie entre deux grilles discrètes: si l'isométrie est atteinte les franges sont dirigées selon la bissectrice extérieure des deux droites discrètes.

Attribuons à la droite discrète d'épaisseur  $\omega$ ,  $\mathcal{D}(a, b, k, \omega, \omega)$ , la **largeur**:

$$l = \frac{\omega}{\sqrt{a^2 + b^2}}$$

En ce sens une grille discrète donne une approximation d'une grille continue.

Il est alors possible de montrer que les lois du Moiré discret **convergent** vers celles du Moiré continu. Regardons celle de la direction des franges.

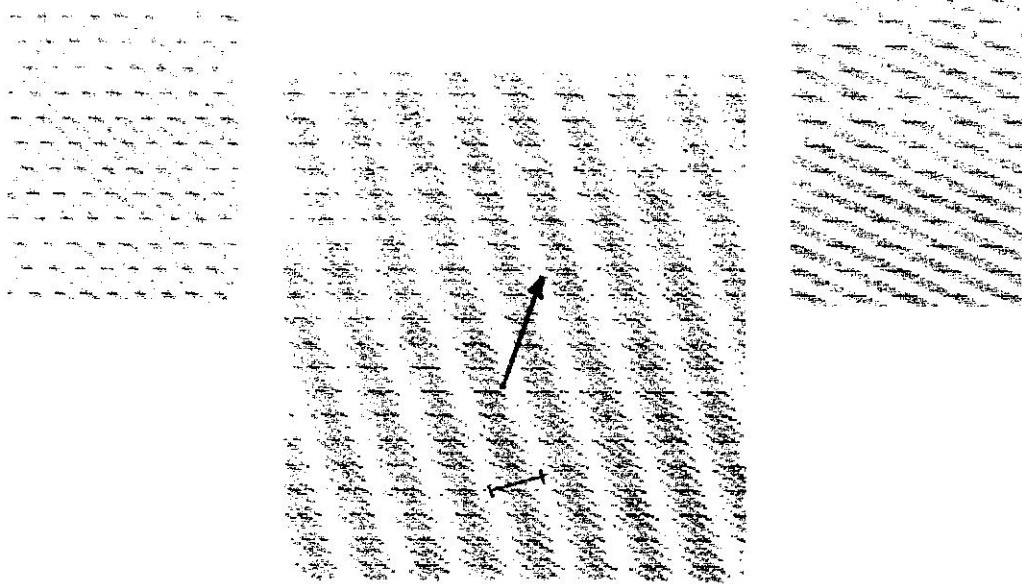


Fig. 3

Moiré des deux grilles d'équations:

$$23 k \leq 4x + 7y < 23 (k+1)$$

$$11 l \leq x + 3y < 11 (l+1)$$

La condition d'isométrie entre les deux grilles discrètes s'écrit:

$$\frac{\omega}{\rho} = \sqrt{\frac{a^2+b^2}{c^2+d^2}}$$

Elle n'a généralement pas de solutions entières  $\omega$  et  $\rho$  mais possède des solutions approchées intéressantes:

$$\frac{\omega}{\rho} = \frac{u}{v_p} \quad p=1,2,3\dots$$

où  $\frac{u}{v_p}$  est la  $p$ -ième réduite du développement en fraction continue de

l'irrationnel  $\sqrt{\frac{a^2+b^2}{c^2+d^2}}$ .

Si  $p$  est assez grand les grilles discrètes sont à peu près isométriques et la direction des franges tend vers celle de la bissectrice extérieure de l'angle des réseaux.

Sous la même hypothèse,  $p \rightarrow \infty$ , l'interfrange tend vers  $\frac{\ell}{\sin(\frac{\alpha}{2})}$  et le niveau de gris moyen tend vers la fonction  $1-|x|$ .

Illustrons cette convergence à l'aide de nos grilles où  $a=4$ ,  $b=7$ ,  $c=1$ ,  $d=3$  l'irrationnel étant  $(13/2)$  et son développement en fraction continue:

$$[2; 1, 1, 4, 1, 1, 4, 1, 1, 4, \dots].$$

Les premières réduites  $3/1$ ,  $5/2$ ,  $23/9$ ,  $28/11$ ,  $51/20$ , nous donnent donc les épaisseurs arithmétiques de grilles qui sont de plus en plus ressemblantes. Là aussi les Moirés associés, représentés sur un même écran, permettent, par l'évolution de la direction de leurs franges, d'apprécier cette convergence vers l'isométrie.

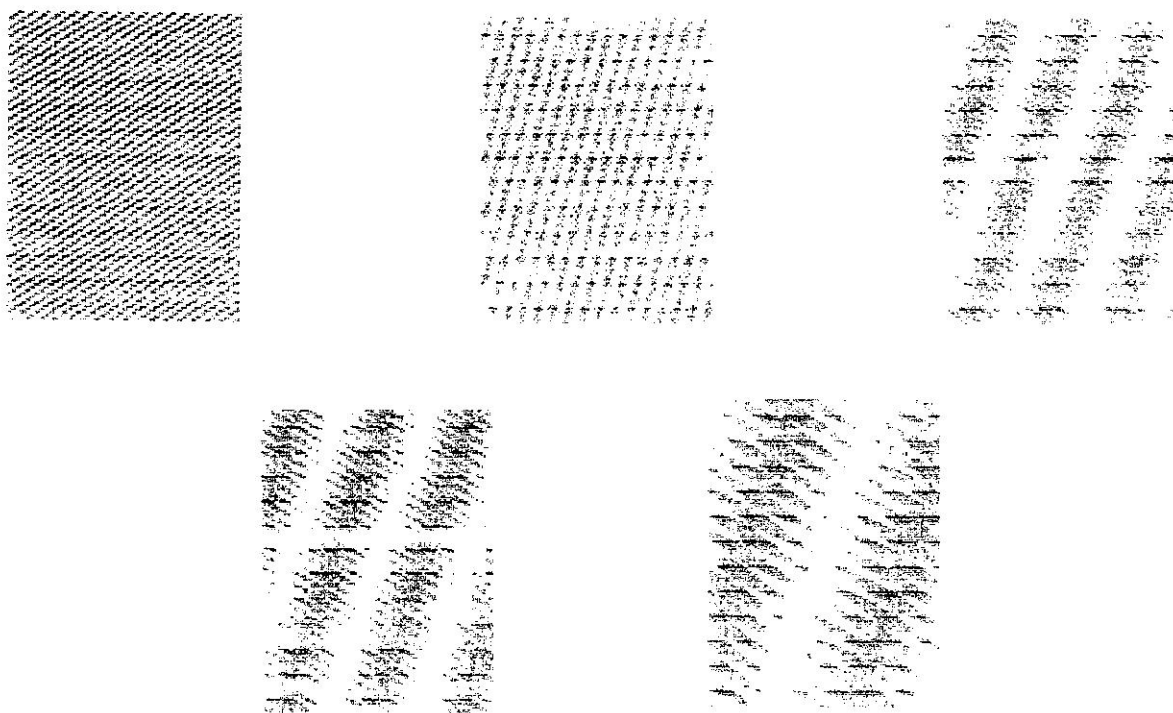


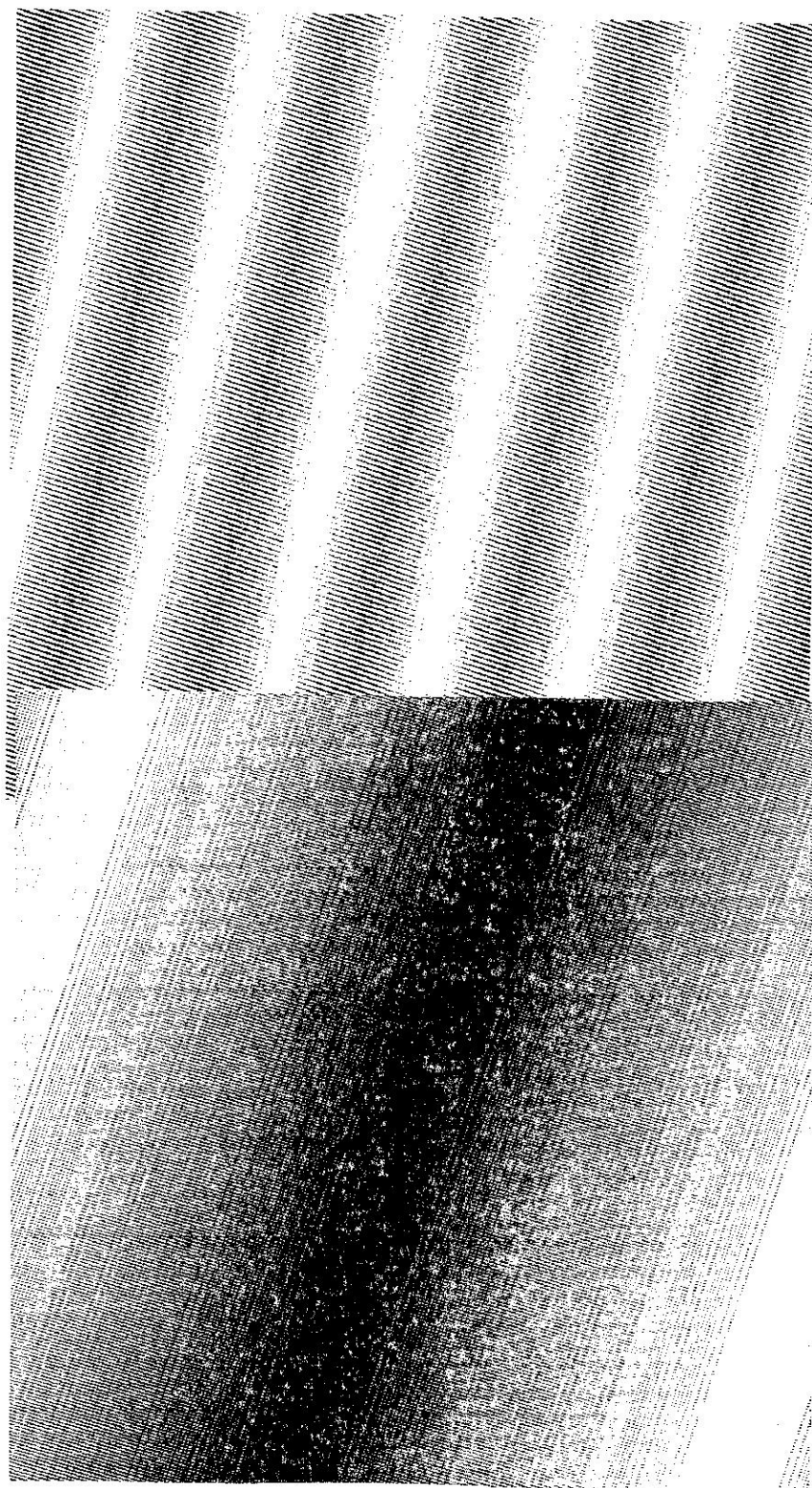
Fig. 4

Moiré des deux grilles de paramètres:

$$a:=4, b:=7, \text{ et } c:=1, d:=3$$

pour  $(w,r) = (3,1), (5,2), (3,9), (28,11), (51,20)$

Nous terminons cette partie en donnant quelques exemples de Moirés de grilles discrètes de directions très voisines. Nous pouvons apprécier la largeur des franges et la variation linéaire prévue du niveau de gris.



Constatons, pour terminer cette partie, que la Géométrie Discrète permet d'aborder avec profit l'étude du phénomène de Moiré. Celui-ci peut servir de référence et d'instrument de mesure même dans ce contexte. Il recèle bien d'autres richesses, tant du point de vue continu que discret que nous espérons exploiter ultérieurement.

TROISIEME PARTIE

LE CALCUL EN NOMBRES ENTIERS

## INTRODUCTION

L'hyperordinateur apporte un cadre théorique nouveau dans l'étude des relations entre le discret et le continu. Sa programmation permet de remplacer les calculs en nombres réels par d'autres, équivalents, dans les modèles finitaires  $R_{\omega, \rho}$  précédents. Cette activité constitue le Calcul en Nombres Entiers. Elle met en évidence qu'avec une base de numération,  $\omega$ , infiniment grande l'arithmétique est équivalente, sans report de retenues, au calcul réel; c'est la virgule fixe à un chiffre. Par contre l'emploi de bases standard, donc d'un nombre infiniment grand de chiffres, nécessite de gérer des reports de retenues encombrants. Mais la puissance des machines actuelles et notre besoin, somme toute limité de précision, montre qu'on peut souvent se contenter d'une arithmétique à deux ou trois chiffres (en base  $\omega=2^{32}$  la précision avoisine les  $10^{30}$ ), or, et c'est là le point essentiel, la gestion des retenues dans de telles arithmétiques fixes n'a rien de très difficile. Si la théorie réclame une puissance infiniment grande pour pouvoir remplacer les calculs réels par de l'arithmétique sans retenues et implique par conséquent une gestion des retenues gigantesque, la pratique montre qu'en fait il n'en est rien et qu'il n'est pas déraisonnable de tenter de gérer directement les retenues et de comparer, en précision et en temps d'exécution, les résultats avec ceux de la virgule flottante. La simple considération de l'hyperordinateur peut conduire à quelques déductions concrètes.

Le Calcul en Nombre Entier aura donc pour principal objectif d'établir les relations permettant de traiter tout calcul réel avec des entiers appartenant à un intervalle  $[0, \omega-1]$ , c'est à dire de "projeter" les algorithmes dans une base de numération et de décrire les reports de retenues pour un petit nombre de chiffres.

En machine le nombre réel est traité comme un bloc d'information minimal; le Calcul en Nombres Entiers repousse cette barrière au niveau des chiffres. Les considérations des temps d'exécution mis à part, la souplesse qui en résulte immédiatement donne un intérêt nouveau aux calculs, même les plus anodins. En effet la traduction en Nombres Entiers d'une "expression arithmétique" (au sens de la Théorie de la Compilation) faisant intervenir les quatre opérations pourra se faire de bien des façons: attribution d'un nombre de chiffres variable aux différentes variables, intervention ou non de tel report de retenue, etc. Une simple expression pourra être traduite de façon plus ou moins efficace, ce qui ouvre l'immense problème de la recherche des conversions optimales.

Sur la question des erreurs deux remarques s'imposent.

o Le Calcul en Nombres Entiers court-circuite la gestion des retenues des virgules fixes (logées dans les compilateurs ou les coprocesseurs), mais il peut évidemment utiliser pour la traduction, le même principe que le compilateur; il donnera alors une formule qui, à précision égale, fournira les mêmes résultats que l'arithmétique flottante. La grande différence c'est qu'il peut fournir un très grand nombre d'autres formules arithmétiques, certaines pouvant être plus mauvaises ou meilleures que la formule du flottant. Il n'y a pas, pour l'instant, de théorème général conduisant toujours à un meilleur résultat en Nombres Entiers. Par contre certaines démarches théoriques, hors d'atteinte d'un compilateur, comme le contrôle des points entiers les plus voisins d'une fonction donnée, permettent de fournir des algorithmes plus efficaces.

o La virgule flottante, comme tous les processus de calcul approché, s'accompagnent d'erreurs d'arrondi. Si, dans un cas précis, le calcul en nombres entiers a pu fournir une formule efficace, l'algorithme qui en résulte, n'utilisant dès lors que des calculs entiers, n'est pas entaché de ce phénomène de dérive; il devient numériquement plus stable. Il est alors possible de localiser dans son expression les termes qui, une fois supprimés ou modifiés, la feront se comporter comme la formule flottante associée.

Toutefois ces avantages du Calcul en Nombres Entiers qui permettent d'accélérer les calculs ou d'implanter des algorithmes "réels" dans des composants rustiques ne sont pas les seuls, loin s'en faut. Ils ramènent surtout les problèmes du Continu Mathématique à d'autres qui ne dépendent plus que d'une **quantité d'information finie** contenue dans quelques paramètres et variables entières. Ceci ouvre aussi une autre perspective immense: analyser les problèmes continus en fonction de cette arithmétique sous-jacente. Il ne s'agit pas moins que d'exprimer arithmétiquement les lois du Continu. On reste d'ailleurs fasciné dès que l'on traduit graphiquement les résultats obtenus par cette méthode.

Jusqu'à présent notre expérience de cette technique ayant surtout porté sur les applications graphiques et l'intégration des équations différentielles, c'est dans ces domaines que nous puiserons nos illustrations. Notre démarche conduit à des algorithmes d'approximation entière de polynômes à coefficients réels et de tracé de solutions d'équations différentielles en base  $\omega$  donnant pour chacune d'elles une suite de points à coordonnées entières (à l'échelle  $\omega$ ) infiniment voisine. Nos algorithmes sont tout à fait comparables aux algorithmes de Bresenham utilisés en graphisme.

# I LA GESTION DES RETENUES ET LA CONVERSION DES ALGORITHMES.

## 1 Les entiers en base $\omega$ et la gestion des retenues.

Lorsque nous remplaçons les nombres réels par des entiers rapportés à une unité  $\omega$  infiniment grande également base de numération tout entier  $n$  s'écrit

$$n = a_k \omega^k + \dots + a_1 \omega + a_0 \quad \text{où } a_i < \omega \quad (1)$$

Pour réduire les confusions avec l'usage de la base décimale nous utiliserons peu le symbole

$$a_k a_{k-1} \dots a_1 a_0$$

traditionnellement associé à (1).

Tout réel "limité" sera représenté, dans ce système, par un nombre à deux chiffres  $a_1 a_0$  où  $a_1$  est standard. Par là les calculs sur les réels peuvent être remplacés par d'autres portant sur des nombres à deux chiffres si la base est assez grande. Quoique ce point de départ soit le même que celui qui conduit au choix et à l'élaboration des arithmétiques à virgule flottante notre route se sépare immédiatement de celle-ci. Au lieu de traduire automatiquement toutes les opérations arithmétiques portant sur des quantités réelles intervenant dans une expression ou un algorithme nous les explicitons directement sur leurs chiffres dans la base choisie. Une justification de nature générale est nécessaire.

Soit  $L_\omega$  ( $L$  pour limité) la collection des entiers  $a_1 \omega + a_0$  où  $a_1$  est standard.

Un élément  $x = a_1 \omega + a_0$  de  $L_\omega$  est infiniment petit si et seulement si  $a_1$  est nul et  $a_0$  est infiniment petit devant  $\omega$ .

Les opérations mentionnées étant celles introduites au chapitre 1 la proposition ci-dessous précise les propriétés de stabilité de  $L_\omega$ .

### proposition 1

Si  $i$  et  $j$  sont dans  $L_\omega$  alors la somme  $i+j$ , la différence  $i-j$ , le produit  $i \cdot j$  et, si  $j$  n'est pas infiniment petit, le quotient  $i/j$  sont dans  $L_\omega$ .

Cette proposition montre qu'il est possible de remplacer les calculs sur les

réels par des calculs sur des entités plus pauvres comme les nombres à deux chiffres  $a_1 a_0$  de  $L_\omega$ ; cette arithmétique à virgule fixe simplifiée peut être utilisée comme modèle idéal du corps des réels pour ordinateur. Bien que l'hypothèse  $\omega$  infiniment grand reste théorique elle n'empêche pas  $L_\omega$  de servir de cadre pour traduire les mathématiques et analyser le comportement d'un ordinateur dans sa simulation du continu. Nous pouvons également mettre à l'épreuve, en les exécutant, les algorithmes que nous obtenons par cette voie,  $\omega$  n'étant plus infiniment grand mais simplement "grand" et les comparer aux méthodes classiques. Les résultats sont généralement bons et les algorithmes rapides surtout parce que nous évitons les nombreux calculs, transparents à l'utilisateur, de gestion des retenues nécessaires à l'arithmétique flottante (ou fixe); ici nous prenons ceux-ci en charge tout en nous permettant, avantage important, d'intervenir dans les algorithmes par des approximations judicieuses.

L'arithmétique de  $L_\omega$  peut s'avérer insuffisante lorsque nous quittons le domaine formel pour celui des applications effectives, une généralisation des arithmétiques à multiprécision peut alors être utilisée. Nous ne développerons pas ici cette théorie.

## 2 La conversion d'une formule.

Les compilateurs traduisent usuellement, chacune des 4 opérations intervenant dans une expression arithmétique, par une procédure fixée. Ici nous nous chargeons de ce travail. Le seul problème posé, en ce qui concerne les opérations  $+$ ,  $-$ ,  $\times$ , est de gérer les retenues; la division rajoute quelques difficultés propres. En suivant cette voie nous constatons qu'une formule donnée admet plusieurs versions entières différentes. C'est un enrichissement offert à l'utilisateur la méthode est une source d'algorithmes quasiment inépuisable.

Examinons pour commencer le cas d'une somme.

Quelques notations simplifierons l'exposé. Si  $n$  est un entier quelconque, l'égalité de division euclidienne par  $\omega$  peut s'écrire

$$n = \left[ \frac{n}{\omega} \right] \omega + \left\{ \frac{n}{\omega} \right\} \quad (2)$$

où  $\left[ \frac{n}{\omega} \right]$  représente le quotient de la division de l'entier  $n$  par  $\omega$  et  $\left\{ \frac{n}{\omega} \right\}$  son reste;  $[x]$  désignant la partie entière de  $x$ . Si dans un contexte donné la référence à  $\omega$  est claire nous nous permettrons d'alléger les notations

suivantes en remplaçant  $\left[ \frac{n}{\omega} \right]$  par  $[n]$  et  $\left\{ \frac{n}{\omega} \right\}$  par  $\langle n \rangle$ . Ces dernières seront qualifiées de notations simplifiées.

Soit  $n$  un entier quelconque, son expression en base  $\omega$  est donnée par

$$[.[[n/\omega]/\omega]./\omega]\omega^k + \{.[[n/\omega]/\omega]./\omega\}\omega^{k-1} + \dots + \langle n/\omega \rangle \quad (3)$$

où le coefficient de  $\omega^p$  comporte  $p$  symboles de partie entière  $[ ]$  et un symbole  $\{ \}$  de reste, celui de  $\omega^k$   $k$  crochets uniquement.

### 3 Expression d'une somme en base $\omega$ .

Si  $a_0, a_1, \dots, a_n$  sont des entiers  $\langle \omega$ , i.e. des chiffres de la base de numération utilisée, l'entier  $\left[ \frac{a_0 + a_1 + \dots + a_n}{\omega} \right]$  représente la retenue de la somme  $a_0 + a_1 + \dots + a_n$  dans ce système. Autrement dit la relation évidente

$$a_0 + a_1 + \dots + a_n = \left[ \frac{a_0 + a_1 + \dots + a_n}{\omega} \right] \omega + \left\{ \frac{a_0 + a_1 + \dots + a_n}{\omega} \right\}$$

exprime les chiffres de la somme lorsque  $a_0 + a_1 + \dots + a_n < \omega^2$ . Si la somme dépasse  $\omega^2$  nous pouvons rajouter, en utilisant (3), les termes requis traduisant les retenues suivantes.

### 4 Calcul des monômes en base $\omega$ .

Dans  $R_\omega$  les monômes  $\alpha x^n$  sont remplacés par les fonctions arithmétiques  $\left[ \frac{ai^{n+1}}{\omega^n} \right]$ . La croissance rapide des fonctions puissance réclame vite des capacités de calcul importantes. Cette question est analysée dans ce paragraphe.

La discrétisation des fonctions monômes de la forme  $\alpha x^n$ , où  $\alpha$  et  $x$  sont réels, est une première étape vers une version discrète des polynômes.

Remplaçons  $\alpha$  par un entier  $a$  de  $R_\omega$ , de sorte que  $[a/\omega] = \alpha$ , la trace macroscopique de la fonction  $i \mapsto \left[ \frac{ai^{n+1}}{\omega^n} \right]$  est, bien entendu, la fonction  $\alpha x^{n+1}$ . Nous désignerons sous le nom de monôme arithmétique ou  $s$ -monôme une telle fonction discrète. Le problème consiste à déterminer cette suite d'entiers, lorsque  $i$  varie, sans qu'aucun calcul intermédiaire ne dépasse  $\omega^2$ .

Si  $a$  et  $i$  sont deux entiers inférieurs à  $\omega$  leur produit  $ai$  peut dépasser  $\omega$  et

l'on peut écrire, en utilisant (2):

$$ai = \left[ \frac{ai}{\omega} \right] \omega + \left\{ \frac{ai}{\omega} \right\} \quad (4)$$

ce qui nous donne la partie principale de  $ai$  dans la base  $\omega$ . L'exemple suivant sera  $ai^2$ ; en multipliant (4) par  $i$  nous obtenons

$$ai^2 = \left[ \frac{ai}{\omega} \right] \omega i + \left\{ \frac{ai}{\omega} \right\} i \quad (5)$$

$$ai^2 = \left[ \left[ \frac{ai}{\omega} \right] \frac{\omega i}{\omega} + \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right] \omega + \left\{ \left[ \frac{ai}{\omega} \right] \frac{\omega i}{\omega} + \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right\} \quad (6)$$

qui se simplifie en

$$ai^2 = \left[ \frac{ai}{\omega} \right] i \omega + \left\{ \left[ \frac{ai}{\omega} \right] \frac{i}{\omega} \right\} \omega + \left\{ \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right\} \quad (7)$$

Dans cette dernière relation seul le terme  $\left[ \frac{ai}{\omega} \right] i$  n'est pas un chiffre de la base  $\omega$ ; nous appliquons à nouveau (2) qui donne

$$\left[ \frac{ai}{\omega} \right] i = \left[ \left[ \frac{ai}{\omega} \right] \frac{i}{\omega} \right] \omega + \left\{ \left[ \frac{ai}{\omega} \right] \frac{i}{\omega} \right\} \quad (8)$$

et que nous pouvons reporter dans (7) pour obtenir l'expression définitive cherchée.

$$ai^2 = \left[ \left[ \frac{ai}{\omega} \right] \frac{i}{\omega} \right] \omega^2 + \left\{ \left[ \frac{ai}{\omega} \right] \frac{i}{\omega} \right\} \omega + \left[ \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right] \omega + \left\{ \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right\} \quad (9)$$

Celle-ci nous montre que le chiffre dominant est la somme de deux entiers:

$$p = \left[ \left[ \frac{ai}{\omega} \right] \frac{i}{\omega} \right] \quad \text{ou partie principale}$$

et la retenue, quotient entier, par  $\omega$ , de la somme

$$r = \left\{ \left[ \frac{ai}{\omega} \right] \frac{i}{\omega} \right\} + \left[ \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right]$$

Nous avons montré sur cet exemple que la partie entière de  $\frac{ai^2}{\omega^2}$  est égale à  $p +$

$[r/\omega]$ , c'est à dire

$$\left[ \frac{ai^2}{\omega^2} \right] = \left[ \left[ \frac{ai}{\omega} \right] \frac{i}{\omega} \right] + \left[ \frac{\left\{ \left[ \frac{ai}{\omega} \right] \frac{i}{\omega} \right\} + \left\{ \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right\}}{\omega} \right] \quad (10)$$

Nous pouvons également suivre un chemin un peu différent pour calculer  $\left[ \frac{ai^2}{\omega^2} \right]$ . Partons de (5) en extrayant cette fois la partie significative du plus petit terme  $\left\{ \frac{ai}{\omega} \right\} i$  :

$$\left\{ \frac{ai}{\omega} \right\} i = \left[ \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right] \omega + \left\{ \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right\} \quad (11)$$

ce qui conduit à une nouvelle version de (5):

$$ai^2 = \left[ \left[ \frac{ai}{\omega} \right] i + \left[ \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right] \right] \omega + \left\{ \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right\} \quad (12)$$

Nous pouvons extraire maintenant la partie la plus significative du coefficient de  $\omega$ ; il vient:

$$ai^2 = \left[ \frac{\left[ \frac{ai}{\omega} \right] i + \left[ \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right]}{\omega} \right] \omega^2 + \left\{ \frac{\left[ \frac{ai}{\omega} \right] i + \left[ \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right]}{\omega} \right\} \omega + \left\{ \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right\} \quad (13)$$

montrant que

$$\left[ \frac{ai^2}{\omega^2} \right] = \left[ \frac{\left[ \frac{ai}{\omega} \right] i + \left[ \left\{ \frac{ai}{\omega} \right\} \frac{i}{\omega} \right]}{\omega} \right] \quad (14)$$

ce qui semble différent de la première expression (10) trouvée plus haut; ces deux expressions sont en fait égales comme on peut le constater en appliquant le lemme suivant.

lemme

Si a et b sont deux entiers on a la relation

$$\left[ \frac{a+b}{\omega} \right] = \left[ \frac{a}{\omega} \right] + \left[ \frac{\left\{ \frac{a}{\omega} \right\} + b}{\omega} \right] \quad (15)$$

La démonstration est évidente.

La relation (13) est la plus intéressante pour le calcul sur machine à condition que la division "entière" donnant le quotient et le reste dans le même cycle soit accessible. Par contre la relation (10) se généralise assez facilement et conduit à une identité intéressante.

proposition 2 (formule des retenues descendantes)

a et i étant deux entiers inférieurs à  $\omega$  on a la relation

$$a_i^{n+1} = [..[ai]i..]\omega^{n+1} + \sum_{\{\}} [..[ai]i..] \omega^n + \dots \quad (16)$$

$$\sum_{\{\{\}}\} [..[ai]i..] \omega^{n-1} + \dots + \sum_{[]} \{..[ai]i..]\omega + \{..[ai]i..}$$

dans laquelle chaque terme de la somme contient n symboles [] ou {}, les "indices" de sommation indiquant que l'on doit prendre toutes les expressions contenant une paire {} puis toutes les expressions contenant deux paires emboîtées d'accollades etc.. Les nombres de termes de ces sommes sont donnés par les coefficients binomiaux  $\binom{n+1}{p}$ .

Nous déduisons de (16) des valeurs approchées de la partie entière  $\left[ \frac{a_i^{n+1}}{\omega^n} \right]$ :

$$\left[ \frac{a_i^{n+1}}{\omega^n} \right] \sim [..[ai]i..] \quad (17)$$

$$\left[ \frac{a_i^{n+1}}{\omega^n} \right] \sim [..[ai]i..] + \left[ \sum_{\{\}} [..[ai]i..] \right] \quad (17')$$

permettant de définir les s-polynômes de façon très commode pour le calcul sur ordinateur.

#### Remarque

La première relation ne tient pas compte des retenues d'ordre 1,2,3,... alors que la deuxième ne prend en compte que celle du premier ordre. La relation exacte pourrait être obtenue à partir de (16) mais le résultat suivant la rend

moins utile.

### théorème 3

Pour tout entier standard  $n$  on a, au sens de la  $s$ -topologie:

$$\left[ \frac{ai^{n+1}}{\omega^n} \right] \sim [..[ai]i..] \quad (18)$$

le symbole  $[]$  du terme de droite ayant le sens introduit dans la remarque 1 ci-dessus.

### démonstration

Toutes les sommes intervenant dans (16) ne contiennent qu'un nombre standard de termes, donc infiniment petit devant  $\omega$ . Les retenues que chaque somme induit sont donc des entiers négligeables.

Ceci prouve que sous l'hypothèse  $\omega$  infiniment grand nous pouvons utiliser des approximations très simples des monômes, par contre, si nous simulons ces valeurs sur ordinateur en employant des valeurs de  $\omega$  standard (16) permet d'atteindre la valeur exacte de  $\left[ \frac{ai^{n+1}}{\omega^n} \right]$  dont (17) est une approximation d'ordre 0 et (17') une approximation à l'ordre 1; d'autres approximations intermédiaires apparaissent de façon évidente chacune conduisant directement à un algorithme.

### Les différences

$$\left[ \frac{ai^{n+1}}{\omega^n} \right] - [..[ai]i..]$$

sont analogues à des erreurs d'arrondi sur le calcul de  $\left[ \frac{ai^{n+1}}{\omega^n} \right]$ . La relation (16) permet d'en faire un traitement théorique et même si besoin est d'y apporter des corrections.

### Remarque

La formule (16) permet d'obtenir, pour la valeur d'un monôme une expression exacte comme si nous utilisions une arithmétique à multiprécision; plus généralement nous pouvons "simuler" des multiprécisions variables, à notre gré, à l'intérieur d'une expression arithmétique quelconque. Ceci sera amplement repris dans le §9 sur l'évaluation d'un polynôme.

5 Le produit  $a\left(1 + \frac{x}{\omega}\right)^n$  et l'exponentielle arithmétique.

Nous pouvons aborder la fonction exponentielle à partir de l'étude du produit  $a\left(1 + \frac{x}{\omega}\right)^n$  ou, ce qui est équivalent, à partir de la solution  $a\left(\frac{\omega + x}{\omega}\right)^n$  de l'équation aux différences finies associée à l'équation différentielle  $y' = y$  (cf. § 2.4). Nous devons alors déterminer l'entier

$$\left[ \frac{a(\omega + x)^n}{\omega^n} \right]$$

ce qui, visiblement, n'est pas très différent de l'étude des monômes du paragraphe précédent sinon que l'exposant  $n$ , ici, peut être non standard. Nous obtiendrons une approximation d'ordre 1 de l'exponentielle arithmétique par la relation:

$$\left[ \frac{a(\omega + x)^n}{\omega^n} \right] \sim [..[a(\omega+x)](\omega+x)..] + \left[ \sum_{\{ \}} [..[a(\omega+x)](\omega+x)..] \right]$$

où nous utilisons encore la convention du paragraphe précédent concernant les  $[]$  et  $\{ \}$ .

Cette formule ainsi que toutes celles que nous pourrions écrire en tenant compte des diverses retenues permet d'évaluer la fonction exponentielle en un point quelconque en n'effectuant que des divisions entières sur des nombres inférieurs à  $\omega^2$ . Si  $n$  est infiniment grand mais négligeable devant  $\omega$  l'approximation précédente est infinitésimale.

6 Les monômes  $\left[ \frac{a_0 a_1 \dots a_n}{\omega^n} \right]$ .

Le problème du § précédent est un cas particulier de l'évaluation de l'entier

$$\left[ \frac{a_0 a_1 \dots a_n}{\omega^n} \right]$$

où  $a_0, a_1, \dots, a_n$  sont  $n+1$  entiers  $\langle \omega$  donnés, sans qu'aucun calcul intermédiaire ne dépasse  $\omega^2$ . Le traitement donné ci-dessus s'adapte sans difficulté.

proposition 4 (formule des retenues descendantes pour un produit)

$a_0, \dots, a_n$  étant  $n+1$  entiers inférieurs à  $\omega$  on a la relation

$$a_0 \dots a_n = [..[a_0 a_1] a_2 ..] \omega^n + \sum_{\{\}} [..[a_0 a_1] a_2 ..] \omega^{n-1} + \dots + \sum_{\{\{\}} \{ \}} [..[a_0 a_1] a_2 ..] \omega^{n-2} + \dots + \sum_{\{ \}} [..[a_0 a_1] a_2 ..] \omega + \{..[a_0 a_1] ..\} \quad (19)$$

$$\sum_{\{\{\}} \{ \}} [..[a_0 a_1] a_2 ..] \omega^{n-2} + \dots + \sum_{\{ \}} [..[a_0 a_1] a_2 ..] \omega + \{..[a_0 a_1] ..\}$$

où les symboles ont la même signification que dans la formule (15).

Nous en déduisons l'expression approchée suivante de l'entier  $\left[ \frac{a_0 a_1 \dots a_n}{\omega^n} \right]$  en divisant les deux membres de (18) par  $\omega^n$  et en ne retenant que les deux premiers termes:

$$\left[ \frac{a_0 a_1 \dots a_n}{\omega^n} \right] \sim [..[a_0 a_1] a_2 ..] + \frac{\sum_{\{\}} [..[a_0 a_1] a_2 ..] \omega^{n-1}}{\omega} \quad (20)$$

Comme avant, l'approximation a un sens rigoureux dans  $R_\omega$ ; nous laissons la formulation précise au lecteur.

Dans cette formule le premier terme  $[..[a_0 a_1] a_2 ..]$  est la partie principale, analogue à la mantisse d'un réel traditionnel de précision fixée; le deuxième terme est, si l'on peut dire, le terme correctif principal ou premier chiffre après la virgule. Dans l'approche ordinaire du calcul numérique ce terme correctif serait atteint si nous travaillions en précision étendue. Cette expression est importante car elle permet l'atténuation des erreurs d'arrondi de l'expression de la partie principale.

## II POLYNOMES EN NOMBRES ENTIERS.

### 1 Les formules différentielles

Il existe de nombreuses situations réclamant le calcul d'un grand nombre de valeurs successives d'une fonction : intégration, équations différentielles etc. La méthode précédente n'est pas la mieux adaptée surtout si la fonction est régulière; dans ce cas les variations sont petites et ne nécessitent pas un traitement aussi complet.

Nous allons donner un autre moyen de calcul et l'illustrerons avec des

exemples simples. (Dans cette partie nous n'utiliserons pas les notations simplifiées introduites ci-dessus). Examinons le calcul de  $\left[ \frac{ai}{\omega} \right]$ ; l'entier  $ai$  s'écrivant

$$ai = X_i \omega + Y_i$$

nous allons établir des relations de récurrence entre les  $X_i$ ,  $Y_i$ ,  $X_{i+1}$ , et  $Y_{i+1}$ . Comme  $a(i+1) = ai + a$ , nous avons

$$a(i+1) = X_i \omega + Y_i + a$$

où la somme  $Y_i + a$  peut dépasser  $\omega$  et provoquer une retenue s'ajoutant à  $X_i$ ; cette dernière valant  $\left[ \frac{Y_i + a}{\omega} \right]$  nous obtenons les équations :

$$\begin{cases} X_{i+1} = X_i + \left[ \frac{Y_i + a}{\omega} \right] \\ Y_{i+1} = \left\{ \frac{Y_i + a}{\omega} \right\} \end{cases}$$

permettant de calculer de manière itérative le nombre  $\left[ \frac{ai}{\omega} \right] = X_i$  en effectuant des calculs plus simples que ceux suggérés par la formule  $\left[ \frac{ai}{\omega} \right]$ . L'algorithme précédent donne d'ailleurs un tracé de droites discrètes analogue à ceux que nous avons étudié dans la deuxième partie.

Passons au cas des monomes  $\left[ \frac{ai^2}{\omega^2} \right]$  qui nous donnerons un moyen de traiter les polynômes de degré 2.

Partons des définitions évidentes:

$$2ai = U_i \omega + V_i \quad \text{et} \quad ai^2 = X_i \omega^2 + Y_i \omega + Z_i$$

et remplaçons  $i$  par  $i+1$ , les équations suivantes en résultent facilement,

$$\begin{aligned} 2a(i+1) &= U_i \omega + V_i + 2a \\ a(i+1)^2 &= X_i \omega^2 + (Y_i + U_i) \omega + Z_i + V_i + a \end{aligned}$$

ainsi que les relations de récurrence

$$\begin{cases} X_{i+1} = X_i + \left[ Y_i + U_i + \left[ \frac{Z_i + V_i + a}{\omega} \right] \right] \\ Y_{i+1} = \left\{ Y_i + U_i + \left[ \frac{Z_i + V_i + a}{\omega} \right] \right\} \\ Z_{i+1} = \left\{ \frac{Z_i + V_i + a}{\omega} \right\} \end{cases}$$

$$\begin{cases} U_{i+1} = U_i + \left[ \frac{V_i + 2a}{\omega} \right] \\ V_{i+1} = \left\{ \frac{V_i + 2a}{\omega} \right\} \end{cases}$$

qui permettent de calculer de façon itérative, concurremment à (13),  $\left[ \frac{ai^2}{\omega^2} \right]$ . Ce dernier algorithme n'utilise que des additions et quelques divisions par l'unité  $\omega$ .

Donnons maintenant, à titre d'indication, les relations de récurrence permettant de déterminer itérativement le monôme  $\left[ \frac{ai^3}{\omega^3} \right]$ . Posons

$$3ai = R_i \omega + S_i$$

$$3ai^2 = U_i \omega^2 + V_i \omega + W_i$$

$$ai^3 = X_i \omega^3 + Y_i \omega^2 + Z_i \omega + T_i$$

Reprenons ici l'usage des notations simplifiées

$$[x] = [x/\omega] \text{ et } \{x\} = x - [x/\omega]\omega.$$

Les relations cherchées s'obtiennent immédiatement comme dans les exemples précédents:

$$R_{i+1} = R_i + [S_i + 3a]$$

$$S_{i+1} = \{S_i + 3a\}$$

$$U_{i+1} = U_i + [V_i + 2R_i + [W_i + 2S_i + 3a]]$$

$$V_{i+1} = \{V_i + 2R_i + [W_i + 2S_i + 3a]\}$$

$$W_{i+1} = \{W_i + 2S_i + 3a\}$$

$$X_{i+1} = X_i + [Y_i + U_i + [Z_i + V_i + R_i + [T_i + W_i + S_i + a]]]$$

$$Y_{i+1} = \{Y_i + U_i + [Z_i + V_i + R_i + [T_i + W_i + S_i + a]]\}$$

$$Z_{i+1} = \{Z_i + V_i + R_i + [T_i + W_i + S_i + a]\}$$

$$T_{i+1} = \{T_i + W_i + S_i + a\}$$

Le lecteur pourra constater que la complexité de ces algorithmes augmente très rapidement bien que leur exécution reste rapide.

Nous pouvons, heureusement, faire quelques approximations, comme l'oubli des  $R_i, S_i, U_i, V_i, W_i$  donnant un système de récurrences simplifié:

$$X_{i+1} = X_i + [Y_i + [Z_i + [T_i + a]]]$$

$$Y_{i+1} = \{Y_i + U_i + [Z_i + [T_i + a]]\}$$

$$Z_{i+1} = \{Z_i + [T_i + a]\}$$

$$T_{i+1} = \{T_i + a\}$$

donnant une autre évaluation de  $\left[\frac{ai^3}{\omega^3}\right]$  dont la précision peut être suffisante dans certaines circonstances.

## 2 Evaluation des polynômes réels: Taylor en Nombres entiers.

L'évaluation d'un monôme en nombres entiers nous a conduit à expliciter les retenues des multiplications; si plusieurs monômes sont ajoutés il faut aussi tenir compte de celles des additions; l'algorithme auquel ceci conduit est peu efficace. Il est plus intéressant d'aborder le problème de l'évaluation d'un polynôme en base  $\omega$  par d'autres méthodes. Nous en examinerons deux distinctes, la première utilisant la formule de Taylor, la deuxième le parenthésage de Horner.

Pour évaluer un polynôme à coefficients réels d'une variable réelle

$$R(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0$$

par des entiers nous commençons par effectuer une homothétie de rapport  $\omega$  dans les deux directions du système de coordonnées en posant  $x = \frac{i}{\omega}$  et en multipliant  $R(x)$  par  $\omega$ ; nous pouvons ensuite remplacer pour  $i=0,1,\dots,n$  le coefficient  $\omega\alpha_i$  par sa partie entière notée  $a_i$ . Nous obtenons la relation approchée:

$$\omega R(x) \sim a_n \frac{i^n}{\omega^n} + a_{n-1} \frac{i^{n-1}}{\omega^{n-1}} + \dots + a_1 \frac{i}{\omega} + a_0$$

En posant

$$P(i) = a_n i^n + a_{n-1} \omega i^{n-1} + \dots + a_1 \omega^{n-1} i + a_0 \omega^n \quad (1)$$

l'évaluation à des infiniment petits près de  $R(x)$  équivaut au calcul des parties entières

$$\left[ \frac{P(i)}{\omega^{n+1}} \right]$$

Si nous nous préoccupons du calcul effectif de ces valeurs sur machine nous observons que des ordres de grandeurs différents interviennent simultanément, nous pouvons faire un traitement adapté grâce à  $R_\omega$  en utilisant la juste quantité d'information nécessaire à chaque terme.

Supposons que  $i$  et chaque coefficient  $a_i$  de (1) soit un chiffre du système de base  $\omega$ , chaque monôme de (1) est de l'ordre de  $\omega^n$ ; associons à l'élément  $P(i)$  de  $R_\omega$  l'entier

$$P(i) = X_n \omega^n + X_{n-1} \omega^{n-1} + \dots + X_1 \omega + X_0 \quad (2)$$

remarque: ici les chiffres sont entendus dans un sens plus large qu'habituellement, ils sont de signe quelconque, leur valeur absolue est strictement inférieure à  $\omega$ . L'obligation de suivre strictement la règle des chiffres de même signe est largement superflue tant que l'on calcule en machine.

L'évaluation consiste à obtenir les chiffres  $Y_n, Y_{n-1}, \dots, Y_1, Y_0$  de  $P(i+1)$  à partir de ceux de  $P(i)$ :  $X_n, X_{n-1}, \dots, X_1, X_0$ , donc donner des relations de récurrence entre ces quantités. L'équation définissant les  $Y_i$

$$P(i+1) = Y_n \omega^n + Y_{n-1} \omega^{n-1} + \dots + Y_1 \omega + Y_0 \quad (3)$$

suggère l'utilisation de la formule de Taylor

$$P(i+1) = P(i) + \frac{P'(i)}{1!} + \dots + \frac{P^{(n)}(i)}{n!} \quad (4)$$

et l'introduction d'entiers de précision inférieure, écrits en base  $\omega$ , pour chaque expression

$$\frac{P^{(k)}(i)}{k!} = X_{n-k}^{(k)} \omega^{n-k} + X_{n-k-1}^{(k)} \omega^{n-k-1} + \dots + X_1^{(k)} \omega + X_0^{(k)} \quad (5)$$

où les indices supérieurs affectés aux chiffres rappellent l'ordre de dérivation; par convention on a  $X_i^{(0)} = X_i$ . Suivant (3) nous noterons comme suit la valeur de  $\frac{P^{(k)}(i+1)}{k!}$  :

$$\frac{P^{(k)}(i+1)}{k!} = Y_{n-k}^{(k)} \omega^{n-k} + Y_{n-k-1}^{(k)} \omega^{n-k-1} + \dots + Y_1^{(k)} \omega + Y_0^{(k)} \quad (6)$$

Il s'agit maintenant d'obtenir des relations de récurrences désirées à partir de (3), (4), (5) et (6) exprimant les  $Y_p^{(k)}$  en fonction des  $X_q^{(i)}$ . En remplaçant dans (4) les  $\frac{P^{(k)}(i)}{k!}$  par leur expression donnée en (5) nous obtenons

$$P(i+1) = X_n \omega^n + (X_{n-1} + X_{n-1}') \omega^{n-1} + (X_{n-2} + X_{n-2}' + X_{n-2}'') \omega^{n-2} \\ \dots \\ + (X_{n-k} + X_{n-k}' + \dots + X_{n-k}^{(k-1)} + X_{n-k}^{(k)}) \omega^{n-k} \\ \dots \\ + (X_0 + X_0' + \dots + X_0^{(n-1)} + X_0^{(n)})$$

qu'il suffit d'écrire correctement dans la base  $\omega$ . Désignons, pour simplifier, par  $S_k$  le coefficient de  $\omega^{n-k}$  dans l'égalité précédente donc

$$S_k = X_{n-k} + X_{n-k}' + \dots + X_{n-k}^{(k-1)} + X_{n-k}^{(k)}$$

Il en résulte que les chiffres de  $P(i+1)$  sont

$$Y_0 = \left\{ \frac{S_0}{\omega} \right\} \\ Y_1 = \left\{ \frac{S_1 + [S_0/\omega]}{\omega} \right\} \text{ que l'on peut encore écrire, pour alléger la présentation,} \\ \text{sous la forme suivante:}$$

$$Y_1 = \left\{ S_1/\omega + [S_0/\omega]/\omega \right\}$$

Plus généralement on a

$$Y_k = \left\{ S_k/\omega + [S_{k-1}/\omega + [S_{k-1}/\omega + [\dots + [S_0/\omega]/\omega \dots]/\omega]/\omega]/\omega \right\} \quad (7)$$

Cette expression indique les calculs à effectuer pour obtenir le  $k$ -ième chiffre de  $P(i+1)$ . Des calculs analogues doivent être conduits simultanément avec les entiers  $\frac{P^{(k)}(i+1)}{k!}$ .

L'égalité de Taylor pour  $\frac{P^{(k)}(i+1)}{k!}$  s'écrit

$$\frac{P^{(k)}(i+1)}{k!} = C_k^k \frac{P^{(k)}(i)}{k!} + C_{k+1}^k \frac{P^{(k+1)}(i)}{(k+1)!} + \dots + C_n^k \frac{P^{(n)}(i)}{n!}$$

où  $C_n^p$  désigne le coefficient binomial.

Posons maintenant

$$S_p^{(k)} = C_k^k X_p^{(k)} + C_{k+1}^k X_p^{(k+1)} + \dots + C_{n-p}^k X_p^{(n-p)} \quad \text{où } 0 \leq p \leq n-k;$$

par convention on a  $S_p^{(0)} = S_p$ . La relation (7) se généralise et devient:

$$Y_p^{(k)} = \left\{ S_p^{(k)} / \omega + [S_{p-1}^{(k)} / \omega + [S_{p-2}^{(k)} / \omega + [\dots + [S_0^{(k)} / \omega] / \omega \dots] / \omega] / \omega \right\} \quad (8)$$

$p = 0, 1, \dots, n-k$

traduisant les récurrences cherchées.

Les valeurs initiales des suites  $X_p^{(k)}$  sont définies à l'aide des coefficients du polynôme  $P(i)$  introduits en (1). Comme la valeur à l'origine de  $\frac{P^{(k)}(0)}{k!}$  vaut  $a_k \omega^{n-k}$  et coïncide avec

$$X_{n-k}^{(k)} \omega^{n-k} + X_{n-k-1}^{(k)} \omega^{n-k-1} + \dots + X_1^{(k)} \omega + X_0^{(k)},$$

par identification,  $a_k$  est la valeur initiale de la suite  $\{X_{n-k}^{(k)}\}$ , les autres suites valant 0 pour  $i=0$ .

L'algorithme s'en déduit facilement, après calcul des  $Y_q^{(1)}$  il suffit de transférer ces valeurs dans les  $X_q^{(1)}$  et d'itérer ce processus.

Les formules de récurrence (8) permettent un calcul itératif exact de  $P(i)$ . Par là nous entendons que par rapport à la valeur  $P(i)$  celle que nous calculons pour  $P(i+1)$  est exacte. L'algorithme est en fait plus précis que le laisse entendre cette première présentation. Nous pouvons initialiser les suites  $\{X_{n-i}^{(k)}\}$ , où  $i > k$ , avec les "décimales" situées après la virgule des quantités étudiées. Tel qu'il est présenté l'algorithme permet, pour un polynôme de degré  $n$  et une base de  $\omega = 10^t$  de calculer rigoureusement  $P(i)$  avec  $t(n+1)$  chiffres (décimaux) significatifs. Les nombres de chiffres, en base  $\omega$ , peuvent sans difficulté être portés à une valeur arbitraire pour  $P(i)$  et  $P^{(k)}(i)/k!$ , conduisant à un algorithme général à précision paramétrable.

Chaque entier associé à  $P(i)$ ,  $P'(i)/1!, \dots$  représente les coefficients du polynôme dans la base algébrique  $1, (X-i), (X-i)^2, \dots$  et notre algorithme est une version en base  $\omega$  à précision variable des formules de Newton. Plus précisément la précision ou longueur vaut 1 pour  $a_n$ , 2 pour  $a_{n-1}, \dots, n+1$  pour le terme constant  $a_0$ ; ici la longueur désigne le nombre de chiffres. Nous pouvons affecter des valeurs initiales compatibles avec ces choix à chacun d'eux. Si nous perturbons l'un des chiffres de la condition initiale nous

rajoutons un polynôme dont le coefficient de degré correspondant est égal à cette perturbation.

### Exemple

Détaillons à titre d'exemple ces relations pour l'évaluation de

$$P(i) = ax^3 + bx^2 + cx + d$$

En simplifiant les notations précédentes nous posons

$$P(i) = X_3 \omega^3 + X_2 \omega^2 + X_1 \omega + X_0$$

$$P(i+1) = Y_3 \omega^3 + Y_2 \omega^2 + Y_1 \omega + Y_0$$

et pour leurs dérivées

$$\frac{P'(i)}{1!} = X_2' \omega^2 + X_1' \omega + X_0'$$

$$\frac{P'(i+1)}{1!} = Y_2' \omega^2 + Y_1' \omega + Y_0'$$

$$\frac{P''(i)}{2!} = X_1'' \omega + X_0''$$

$$\frac{P''(i+1)}{2!} = Y_1'' \omega + Y_0''$$

$$\frac{P'''(i)}{3!} = X_0'''$$

$$\frac{P'''(i+1)}{3!} = Y_0'''$$

Il vient

$$Y_0 = \{(X_0 + X_0' + X_0'' + X_0''')/\omega\}$$

$$Y_1 = \{(X_1 + X_1' + X_1'' + [(X_0 + X_0' + X_0'' + X_0''')/\omega])/\omega\} \quad (9)$$

$$Y_2 = \{(X_2 + X_2' + [(X_1 + X_1' + X_1'' + [(X_0 + X_0' + X_0'' + X_0''')/\omega])/\omega])/\omega\}$$

$$Y_3 = X_3 + [(X_2 + X_2' + [(X_1 + X_1' + X_1'' + [(X_0 + X_0' + X_0'' + X_0''')/\omega])/\omega])/\omega]$$

puis en utilisant les identités de Taylor pour  $\frac{P'(i+1)}{1!}$  et  $\frac{P''(i+1)}{1!}$  nous déduisons les relations

$$\begin{aligned} Y_0' &= \{(X_0' + 2X_0'' + 3X_0''')/\omega\} \\ Y_1' &= \{(X_1' + 2X_1'' + [(X_0' + 2X_0'' + 3X_0''')/\omega])/\omega\} \\ Y_2' &= X_2' + [(X_1' + 2X_1'' + [(X_0' + 2X_0'' + 3X_0''')/\omega])/\omega] \end{aligned} \quad (10)$$

$$\begin{aligned}
 Y_0'' &= \{(X_0'' + 3X_0''')/\omega\} \\
 Y_1'' &= X_1'' + [(X_0'' + 3X_0''')/\omega]
 \end{aligned}
 \tag{11}$$

$P'''(i)$   
 $\frac{\quad}{3!}$  étant le polynôme constant a il n'est pas nécessaire de l'évaluer.

Les valeurs initiales sont données ci-dessous:

$$\begin{aligned}
 X_3 &= d & X_2 &= 0 & X_1 &= 0 & X_0 &= 0, \\
 X_2' &= c & X_1' &= 0 & X_0' &= 0, \\
 X_1'' &= b & X_0'' &= 0, \\
 X_0''' &= a,
 \end{aligned}$$

Appliquons ces relations pour évaluer quelques valeurs de  $P(i)$  pour le polynôme  $3i^3 - 5\omega i^2 + 11\omega^2 i - 32\omega^3$  l'unité  $\omega$  étant prise à 100. Suivant nos conventions précédentes nous associons aux coefficients de  $P$ , dans l'ordre des puissances croissantes, les entiers suivants:

$$\begin{array}{r}
 -32 \ 00 \ 00 \ 00 \\
 P(0) \quad 11 \ 00 \ 00 \\
 \quad \quad \quad -5 \ 00 \\
 \quad \quad \quad \quad 3
 \end{array}$$

que nous disposons, pour la commodité des calculs, comme ci-dessus; ils forment le tableau initial de  $P(0)$ . L'étape suivante de l'algorithme conduisant à  $P(1)$  donne les entiers

$$\begin{array}{r}
 -32 \ 11 \ -5 \ 3 \\
 P(1) \quad 11 \ -10 \ 9 \\
 \quad \quad \quad -5 \ 9 \\
 \quad \quad \quad \quad 3
 \end{array}$$

La première ligne est augmentée de la somme de toutes les lignes inférieures, la deuxième de la somme de la ligne 3 multipliée par 2 et de la ligne 4 multipliée par 3, conformément aux relations (9), (10), (11). Finalement la troisième ligne est augmentée de la quatrième multipliée par 3, la dernière ne subissant aucune modification. Au cours de cette étape aucun calcul n'a dépassé 100 ou -100 les retenues ne sont pas apparues. Le tableau donnant  $P(2)$  vaut

$$\begin{array}{r}
 -32 \ 22 \ -20 \ 24 \\
 P(2) \quad 11 \ -20 \ 36 \\
 \quad \quad \quad -5 \ 18
 \end{array}$$

Celui de P(3) s'obtient directement sans qu'aucun report de retenue n'intervienne

$$\begin{array}{r}
 -32 \ 33 \ -45 \ 81 \\
 P(3) \quad 11 \ -30 \ 81 \\
 \quad \quad \quad -5 \ 27 \\
 \quad \quad \quad \quad 3
 \end{array}$$

Cette fois quelques retenues interviennent, nous laissons au lecteur le soin de refaire ces calculs à la main.

$$\begin{array}{r}
 -32 \ 44 \ -79 \ 92 \\
 P(4) \quad 11 \ -39 \ 44 \\
 \quad \quad \quad -5 \ 36 \\
 \quad \quad \quad \quad 3
 \end{array}$$

des retenues vont à nouveau intervenir au cours de cette étape conduisant à P(5):

$$\begin{array}{r}
 -32 \ 54 \ -22 \ 75 \\
 P(5) \quad 11 \ -48 \ 25 \\
 \quad \quad \quad -5 \ 45 \\
 \quad \quad \quad \quad 3
 \end{array}$$

Le lecteur pourra examiner les diverses retenues, positives ou négatives apparues dans ce dernier calcul.

#### remarques

a) les termes situés sur les diagonales des tableaux précédents, que nous pourrions qualifier de "significatifs" ne sont pas nécessairement des chiffres, ils peuvent croître au delà de  $\omega$  (ou de  $-\omega$ ), ce qui allège un peu les calculs.

b) Dans l'exemple qui vient d'être traité la "précision" sur P(i) est de 8 chiffres significatifs au moins: nombre de chiffres de la première ligne. Nous constatons que l'algorithme gère le nombre de chiffres nécessaires à la connaissance exacte de P(i), ce qui est souvent superflu.

### 3 Les algorithmes approchés.

Parmi les nombreuses approximations que nous pouvons envisager dans l'algorithme précédent les suivantes sont assez naturelles. Nous dirons que l'ordre de précision de l'algorithme (8) est t (où  $1 \leq t \leq n$ ) si les développements utilisés à la place de (6) sont :

$$P(i) = X_t \omega^n + X_{t-1} \omega^{n-1} + \dots + X_1 \omega + X_0 \quad (12)$$

et plus généralement pour  $k \leq n-t$

$$\frac{P^{(k)}(i)}{k!} = X_t^{(k)} \omega^{n-k} + X_t^{(k)} \omega^{n-k-1} + \dots + X_1^{(k)} \omega + X_0^{(k)}$$

les derniers, pour  $k > n-t$  étant

$$\frac{P^{(n-t)}(i)}{(n-t)!} = X_{t-1}^{(n-t)} \omega^{t-1} + X_{t-2}^{(n-t)} \omega^{t-2} + \dots + X_1^{(n-t)} \omega + X_0^{(n-t)}$$

pour finalement se réduire à l'égalité

$$\frac{P^{(n)}(i)}{n!} = X_0^{(n)}$$

lorsque  $k=n$ .

A des adaptations évidentes près les relations (8) se généralisent à ce cas et conduisent à l'algorithme d'évaluation d'ordre  $t$ .

Une disposition pratique s'avère commode pour présenter les calculs dans le cas général; examinons-la pour l'algorithme d'ordre 2. Plaçons, sur la diagonale d'une matrice  $(n+1) \times (n+1)$  les coefficients  $a_0, \dots, a_n$  du polynôme  $P(x)$  de degré  $n$ , dans l'ordre des puissances croissantes:

$$\begin{array}{cccc|c} a_0 & b_0 & c_0 & & \\ & a_1 & b_1 & c_1 & \\ & & \cdot & \cdot & \\ & & & \cdot & \\ & & & & \cdot & \\ & & & & & \cdot & \\ & & & & & & \cdot & \\ & & & & & & & \cdot & c_{n-2} \\ & & & & & & & & \cdot & \\ & & & & & & & & & \cdot & b_{n-1} \\ & & & & & & & & & & \cdot & a_n \end{array}$$

fig 1

et désignons par  $b_0, b_1, \dots, b_{n-1}, c_0, c_1, \dots, c_{n-2}$   $2n-1$  variables que nous disposons sur des parallèles à la diagonale. Au départ ces variables peuvent être initialisées à 0. La première ligne de la matrice représente l'identité

$$P(i) = a_0 \omega^2 + b_0 \omega + c_0$$

analogue à l'égalité (12) précédente. Les lignes suivantes s'interprètent de même.

Si le tableau précédent est le résultat de la  $i$ -ème étape à la suivante nous aurons, en utilisant les notations  $[]$  et  $\{\}$  simplifiées:

$$c_0 = \{c_0 + b_1 + a_2\}$$

$$b_0 = \{b_0 + a_1 + [c_0 + b_1 + a_2]\}$$

$$a_0 = a_0 + [b_0 + a_1 + [c_0 + b_1 + a_2]]$$

$$c_1 = \{c_1 + 2b_2 + 3a_3\}$$

$$b_1 = \{b_1 + 2a_2 + [c_1 + 2b_2 + 3a_3]\}$$

$$a_1 = a_1 + [b_1 + 2a_2 + [c_1 + 2b_2 + 3a_3]]$$

.....

$$c_{n-2} = \{c_{n-2} + C_{n-1}^{n-2} b_{n-1} + C_n^{n-2} a_n\}$$

$$b_{n-2} = \{b_{n-2} + C_{n-1}^{n-2} a_{n-1} + [c_{n-2} + C_{n-1}^{n-2} b_{n-1} + C_n^{n-2} a_n]\}$$

$$a_{n-2} = a_{n-2} + [b_{n-2} + 2a_{n-1} + [c_{n-2} + C_{n-1}^{n-2} b_{n-1} + C_n^{n-2} a_n]]$$

et finalement

$$b_{n-1} = \{b_{n-1} + C_n^{n-1} a_n\}$$

$$a_{n-1} = a_{n-1} + [b_{n-1} + C_n^{n-1} a_n]$$

$$a_n = a_n, \text{ qui reste constant.}$$

Ces relations peuvent être utilisées pour conduire un calcul à la main sur un tableau tel que celui de la fig 1. Elles assurent l'évaluation directe des chiffres dans le système de numération choisi de  $P(i+1)$  si ceux de  $P(i)$ ,  $P'(i)/i!, \dots$  sont connus.

Nous pouvons considérer l'algorithme (8) comme une évaluation d'un polynôme à l'aide de multiprécisions distinctes simultanées; les algorithmes approchés précédents offrent ainsi des possibilités supplémentaires très utiles pour les applications pratiques. Le cas de l'ordre 1 mérite d'ailleurs un traitement particulier.

#### 4 L'algorithme d'évaluation d'ordre 1 des polynômes

Quelques situations nécessitent un traitement d'un grand nombre de valeurs successives d'un polynôme  $P(x)$  de degré  $n$ ; l'algorithme d'ordre 1 que nous pouvons déduire du cas général précédent est bien adapté à celles-ci. Exprimons, dans la base  $\omega$ , les éléments différentiels en  $i$  avec des notations simplifiées:

$$P(i) = X_0 \omega^n + dX_0 \omega^{n-1}$$

$$\frac{P'(i)}{1!} = X_1 \omega^{n-1} + dX_1 \omega^{n-2}$$

.....

$$\frac{P^{(n)}(i)}{n!} = X_n$$

et en i+1:

$$P(i+1) = Y_0 \omega^n + dY_0 \omega^{n-1}$$

$$\frac{P'(i+1)}{1!} = Y_1 \omega^{n-1} + dY_1 \omega^{n-2}$$

.....

$$\frac{P^{(n)}(i+1)}{n!} = Y_n$$

Les relations de récurrences analogues à (8) sont les suivantes:

$$Y_0 = X_0 + [(X_1 + dX_0)/\omega]$$

$$dY_0 = \{(X_1 + dX_0)/\omega\}$$

$$Y_1 = X_1 + [(2 X_2 + dX_1)/\omega]$$

$$dY_1 = \{(2 X_2 + dX_1)/\omega\}$$

.....

$$Y_i = X_i + [(i+1)X_{i+1} + dX_i]/\omega]$$

$$dY_i = \{(i+1)X_{i+1} + dX_i)/\omega\}$$

.....

$$Y_n = X_n$$

où les [] et {} sont encore utilisées pour le quotient entier et le reste des divisions entières impliquées.

Les calculs indiqués par cet algorithme peuvent, sans difficulté, être conduits à la main. Donnons un petit exemple à partir du polynôme de degré 2  $P(x) = x - x^2$  (en notation traditionnelle). Dans le but de le tabuler en nombres entiers nous transformons  $P(x)$  en posant  $x = i/\omega$ , donnant  $\omega P(i/\omega) = (\omega x - x^2)/\omega$  et introduisons son expression en base  $\omega$  :

$$\omega P(i/\omega) = X_0 \omega^2 + dX_0 \omega$$

puis celle de  $\omega P'(i/\omega)$  où  $P'$  est la dérivée par rapport à  $x$ . D'où l'identité

$$\omega P'(i/\omega)/1! = X_1 \omega + dX_1$$

Finalement celle de  $\omega P''(i/\omega)/2!$ , qui reste constante, vaut  $X_2$ . Prenons  $\omega = 100$ ,  $X_0 = 0$ ,  $X_1 = 100$ ,  $X_2 = -100$ , ce qui correspond aux conditions à l'origine. Les calculs, rassemblés dans le tableau ci-dessous, donnent les éléments différentiels en  $i=0, 1, 2, \dots, 5$ .

$X_0$	$dX_0$	$X_1$	$dX_1$	$X_2$
0	0	100	0	-100
1	0	98	0	-100
1	98	96	0	-100
2	94	94	0	-100
3	88	92	0	-100
4	80	90	0	-100
5	70	88	0	-100
6	58	86	0	-100

La première ligne est constituée par les données; la suivante résulte des calculs ci-dessous:

$X_0 = 0 + [(0+100)/100] = 1$ , le reste de la division étant nul,  $dX_0=0$ ; puis  $X_1 = 100 + [(0-200)/100] = 98$ ; la dernière division ne produisant pas de reste on a  $dX_1=0$ . Les lignes suivantes s'obtiennent de la même façon.

$$\alpha_{p+1}^{p+1} = a_{n-p-1} + [\alpha_p^p i] + \left[ \{\alpha_p^p i\} + \left[ \{\alpha_p^{p-1} i\} + \left[ \dots \left[ \{\alpha_p^1 i\} + [\alpha_p^0 i] \dots \right] \right] \right] \right]$$

Dans un langage de programmation ces relations se traduisent sans difficulté en procédure.

### III EQUATIONS DIFFERENTIELLES EN NOMBRES ENTIERS.

#### 1 Intégration numérique de l'équation $y'=y$ en nombres entiers.

Une nouvelle méthode d'intégration des équations différentielles utilisant les méthodes précédentes va être présentée ci-dessous. Un programme de G. Reeb pour l'équation:

$$y'=y \tag{1}$$

a joué un rôle essentiel, (cf [93]).

La solution de ce problème peut être considérée comme une réponse à des questions pratiques de graphisme sur ordinateur. Une extension de la méthode à des équations différentielles plus générales fournirait un grand nombre d'algorithmes graphiques de type Bresenham. Nous examinerons quelques cas particuliers d'intérêt général en commençant par celui cité plus haut.

Plaçons nous tout d'abord dans  $\mathbb{R}$  pour effectuer une discrétisation de (1); subdivisons l'intervalle  $[0,1]$  en  $\omega$  parties égales par des points

$$x_i = \frac{i}{\omega}$$

et appelons  $y_i$  la valeur de la solution étudiée  $y$  en  $x_i$ . La dérivée est alors approchée par l'expression

$$\frac{y_{n+1} - y_n}{1/\omega}$$

L'équation (1) devient

$$y_{n+1} - y_n = \frac{y_n}{\omega} \tag{2}$$

ou

$$y_{n+1} = \left(1 + \frac{1}{\omega}\right) y_n \tag{3}$$

dont la solution, dépendant de la condition initiale  $y_0$ , est

$$y_n = \left(1 + \frac{1}{\omega}\right)^n y_0 \tag{4}$$

Nous retrouvons le produit du paragraphe 1 précédent auquel nous appliquons un traitement un peu différent.

La relation (3) porte sur des nombres réels; pour travailler avec des nombres entiers nous utiliserons une dilatation de coefficient infiniment grand. Autrement dit nous supposerons  $\omega$  entier infiniment grand et multiplions (3) par  $\omega$ ; il vient

$$\omega y_{n+1} = \omega y_n + y_n \quad (5)$$

dont les termes sont encore des réels.

#### Remarques

i) Nous ne commettrions qu'une erreur infiniment petite en prenant les parties entières de chaque terme de (5). Autrement dit (5) contient une justification théorique de la validité de l'emploi des nombres entiers dans l'intégration numérique des équations différentielles.

ii) La méthode précédente pourrait visiblement être adaptée à des cas beaucoup plus généraux; c'est le souci d'entreprendre une révision générale des méthodes d'intégration numérique qui nous a conduit à commencer par la plus typique des équations.

iii) Nous pouvons réutiliser dans (5) le même procédé pour améliorer la précision. Ces remarques nous amènent à poser

$$Y_n = [\omega y_n]$$

et

$$R_n = [\omega(\omega y_n - Y_n)]$$

où  $[\ ]$  désigne la partie entière.

La relation approchée suivante s'en déduit:

$$\omega y_n \quad Y_n + \frac{R_n}{\omega}$$

ainsi que

$$Y_{n+1} + \frac{R_{n+1}}{\omega} \quad Y_n + \frac{R_n}{\omega} + \frac{Y_n}{\omega} + \frac{R_n}{\omega^2}$$

d'où nous déduisons, en négligeant le terme en  $\frac{R_n}{\omega^2}$ ,

$$Y_{n+1} + \frac{R_{n+1}}{\omega} \quad Y_n + \frac{R_n}{\omega} + \frac{Y_n}{\omega} \quad (6)$$

Les relations de récurrence s'obtiennent en extrayant les parties entières.

$$\begin{cases} Y_{n+1} = Y_n + \left[ \frac{R_n + Y_n}{\omega} \right] \\ R_{n+1} = \left\{ \frac{R_n + Y_n}{\omega} \right\} \end{cases} \quad (7)$$

Mise en oeuvre pratique

Si nous prenons, pour simplifier,  $v=\omega$ , nous pouvons introduire trois suites:  $y_n$ ,  $dy_n$  et  $reste_n$  pour représenter respectivement les progressions de, la solution, son accroissement et de l'erreur. Les relations de récurrence entre elles s'obtiennent sans difficulté

$$y_{n+1} = y_n + dy_n \quad (8)$$

$$dy_{n+1} = (y_{n+1} + reste_n) \text{ div } \omega \quad (9)$$

$$reste_{n+1} = (y_{n+1} + reste_n) \text{ mod } \omega \quad (10)$$

L'équation (8) définit  $dy_n$ , (9) étant la traduction sur cette quantité de (1); (10) est la gestion du reste provenant de deux sources: de l'ordre 1 et de l'ordre 2.

Le programme Pascal suivant traduit ces relations.

```

program Exp;

  Const
    unite=100000;

  Var
    y, dy, i, reste:integer;

  BEGIN
    y:=unite; dy:=0;
    reste:=0;
    for i:=0 to unite do
      begin
        y      :=y+dy;
        dy     :=(y+reste) div unite;
        reste :=(y+reste) mod unite;
      end;
      write(y/unite:10:5);
    END.

```

Sur un micro-ordinateur (16 bits 80286 10 Mhz), ce programme calcule 100000 valeurs successives de la fonction exponentielle, chacune ayant 6 chiffres significatifs, en un peu moins de 40s. Si l'on veut dessiner sur écran des solutions de l'équation il donne de très bons résultats rapidement ( $\omega$  peut être alors choisi autour de 1000).

Examinons maintenant quelques valeurs produites dans un cas simple,  $\omega$  valant 100, le point de départ étant également 100, ce qui correspond à la fonction  $e^x$  elle-même. Celles-ci sont contenues dans le tableau ci-dessous.

$y_n$	$dy_n$	reste <sub>n</sub>
100	1	0
101	1	1
102	1	3
103	1	6
104	1	10
105	1	15
106	1	21
107	1	28
108	1	36
109	1	45
110	1	55
111	1	66
112	1	78
113	1	91
114	2	5
116	1	21
117	1	38

fig. 1

Nous observons que les valeurs produites pour  $y_n$  progressent régulièrement, les incréments étant donnés par la deuxième colonne. La colonne du reste contient en fait la suite de terme général

$$\frac{n(n-1)}{2}$$

conformément à l'identité (6). Mais cette contribution est gérée en ne maintenant dans la dernière colonne que sa valeur modulo  $\omega$  et en reportant dans la deuxième une unité chaque fois que reste<sub>n</sub> atteint ou dépasse  $\omega$ .

Ce procédé n'est pas sans rappeler l'algorithme d'addition de deux entiers dans une base donnée ou encore les techniques dites de "multiprécision"; ici la manière d'utiliser cette précision variable est entièrement à la disposition du programmeur et non plus diffuse dans l'arithmétique flottante du compilateur.

En utilisant les notions de s-dérivabilité évidentes, on peut vérifier que  $y_n$  est s-dérivable.

La justification théorique de l'algorithme se trouve dans le théorème suivant.

## théorème 5

Si  $\rho$  est un entier infiniment petit devant  $\omega$ , la moyenne de la suite  $dy_n$  sur un intervalle de longueur  $\rho$  est infiniment voisine de la dérivée de  $y_n$  en un point de cet intervalle.

### 2 Evaluation rapide de la fonction exponentielle.

Dans les algorithmes précédents les opérations les plus complexes sont des divisions par l'unité  $\omega$ . Si  $\omega$  est une puissance de 2,  $2^k$ , ces opérations peuvent être remplacées par des décalages très rapides. La traduction Pascal de l'algorithme donné par les relations (8) (9) (10) ne tire pas très bien profit des ressources de l'ordinateur. Observons sa simplicité pour  $k=8, 16$  ou  $32$  surtout si nous disposons d'un processeur 8, 16 ou 32 bits. Avec un 8086 si nous prenons pour base  $\omega=2^{16}$  la relation (10) revient à prendre le mot faible de la somme  $y_{n+1} + \text{reste}_n$  calculée sur 32 bits et (9) consiste à en extraire le mot fort. En instructions 8086 nous pouvons écrire la boucle interne de ce calcul.

```
:boucle
      ADD DX,BX
      ADC BX,AX
      ADC AX,0000
      LOOP boucle
```

En initialisant avec  $Ax=1, BX=0, DX=0$  ces instructions conduiront à un calcul très rapide de valeurs de la fonction exponentielle évaluées pour des abscisses régulièrement réparties:  $2^{16}$  itérations sont obtenues en 137 ms (à 10mhz) ce qui est nettement meilleur que le temps de calcul cité plus haut. Il faut dire qu'en matière de temps d'exécutions il est difficile de savoir ce que l'on mesure... La Méthode de Numérisation a l'avantage de fournir des codes traduisibles en langage machine beaucoup plus faciles à étudier et à optimiser. Un dernier avantage réside dans une révision du rôle des coprocesseurs "flottants".

L'algorithme précédent conduit à de très nombreuses variantes selon les situations étudiées. Pour augmenter la précision ds calculs nous pouvons utiliser une base très grande, mais aussi, ce qui est parfois souhaitable, augmenter le nombre de chiffres utilisés. On retrouve par là les classiques méthodes de "multiprécision". Afin de donner une idée précise de ces possibilités examinons l'intégration de l'équation différentielle

$$y' = y \quad (1)$$

en utilisant trois chiffres de poids décroissants,  $C_0, C_1, C_2$ ; elle conduit

alors à l'algorithme suivant.

Algorithme 1

$$\begin{aligned}\bar{C}_2 &= \{C_2 + C_1\} \\ \bar{C}_1 &= \{C_1 + C_0 + [C_2 + C_1]\} \\ \bar{C}_0 &= C_0 + [C_1 + C_0 + [C_2 + C_1]]\end{aligned}\tag{2}$$

Exécutons quelques calculs,  $\omega$  valant 10, en partant des valeurs initiales  $C_0 = 1$ ,  $C_1 = 0$  et  $C_2 = 0$ . Comme nous le verrons plus loin la précision de l'algorithme est une fonction croissante de  $\omega$ ; bien que notre présentation à partir de la valeur  $\omega=10$  soit l'un des cas les plus défavorables, elle est didactiquement commode. Rassemblons les résultats dans un tableau:

i	$C_0$	$C_1$	$C_2$
0	1	0	0
1	1	1	0
2	1	2	1
3	1	3	3
4	1	4	6
5	1	6	0
6	1	7	6
7	1	9	3
8	2	1	2
9	2	3	3
10	2	5	6
11	2	8	1
12	3	0	9

figure 1

L'interprétation se fait en remarquant que pour chaque ligne,  $C_0$ ,  $C_1$  et  $C_2$  sont les chiffres d'une approximation de  $\exp(i/10)$ . Chacune ne dépend que de la précédente contenant une approximation de  $\exp((i-1)/10)$ . Les approximations sont données par la relation:

$$\exp(i/10) \approx C_0 + \frac{C_1}{10} + \frac{C_2}{100}$$

que nous pourrions aussi écrire, en base 10,

$$\exp(i/10) = C_0, C_1 C_2$$

La première ligne du tableau, initialisation de l'algorithme, est en fait la valeur exacte  $\exp(0) = 1,00$ . Pour  $i=10$  nous constatons que l'algorithme fournit la valeur 2.56 comme approximation de  $e$  avec une erreur relative inférieure à  $10\% = 1/\omega$ .

L'algorithme 1 admet une généralisation évidente à un nombre de chiffres quelconque:  $C_0, C_1, C_2, \dots, C_n$ ,  $n \geq 2$ , la base étant  $\omega$

$$\begin{aligned} \bar{C}_n &= \{C_n + C_{n-1}\} \\ \bar{C}_{n-1} &= \{C_{n-1} + C_{n-2} + [C_n + C_{n-1}]\} \\ &\dots\dots\dots \\ \bar{C}_0 &= C_0 + [C_1 + C_0 + [\dots [C_n + C_{n-1}]]] \end{aligned} \quad (3)$$

permettant l'évaluation de  $n+1$  chiffres de valeurs approchées de la fonction exponentielle. Si  $\omega$  est fixé il est facile de constater que la précision des résultats se stabilise et ne peut pas être améliorée en augmentant  $n$ ;  $n=2$  étant un choix convenable.

Passons en revue quelques avantages de cette approche; les calculs à effectuer selon (2) ou (3) ne requièrent aucune arithmétique fixe ou flottante, les seules opérations étant des additions et des divisions par la constante  $\omega$ . Le contrôle de la précision s'effectue via  $\omega$  et le choix du nombre de chiffres,  $n$ ; il est facile de modifier ces paramètres et de regarder ce qui se passe.

Un version Pascal de cet algorithme donne, pour  $\omega=10000$ , 10000 valeurs de l'exponentielle, chacune avec 4 chiffres significatifs au moins, en 0,10 s (à 10 mhz).

### 3 Implémentation de l'Algorithme 1 en langage machine.

L'emploi des entiers permet d'implémenter l'évaluation d'une fonction continue directement dans un processeur rudimentaire qui ne peut exécuter que les 4 opérations entières. Pour atteindre une précision convenable, de 5 à 6 chiffres au cours du calcul il est nécessaire de prendre une valeur de  $\omega$  assez élevée; afin d'accélérer le plus possible les calculs nous prenons  $\omega$  de la forme  $2^k$ . Ceci remplace les **div** et **mod** par des décalages et masquages de mots binaires. Donnons une version langage machine de l'algorithme 1 selon ce principe.

Supposons donc que les  $C_i$  soient des chiffres en base  $2^k$ ; la somme de deux tels chiffres pourra provoquer une retenue d'au plus 1. Généralement les processeurs possèdent deux instructions d'addition analogues à celles du 8086

## ADD X,Y et ADC X,Y

qui ajoutent le contenu de Y à X, avec cumul de la retenue pour la deuxième. Si au cours de l'une de ces opérations un dépassement de la capacité des registres a lieu, la retenue est mise en réserve pour traitement ultérieur.

Si nous disposons de telles additions pour deux entiers de k bits, que nous désignerons encore par ADD X,Y et ADC X,Y, une itération de (1) prend la forme suivante:

```

ADD C2,C1
ADC C1,C0
ADC C0,0
    
```

La première instruction ajoute  $C_1$  au registre contenant  $C_2$ ;  $C_2$  contient alors  $C_2 + C_1 \bmod 2^k$ , la retenue étant mise de côté. La deuxième instruction ajoute  $C_0$  et la retenue éventuelle de la somme antérieure à  $C_1$ . Idem pour le dernier calcul ne nécessitant qu'un éventuel report de retenue. L'algorithme 1 consiste alors à "boucler" autant de fois qu'il le faut sur ces 3 instructions. Les processeurs actuels exécutent ces opérations très rapidement. Notre implantation nous permet très facilement de prévoir le temps d'exécution de notre calcul. Ceci étant rappelé la version 8086 suivante de l'algorithme 1 ne pose pas de difficulté.

```

;prologue
    MOV CX,FFFF
    MOV AX,0001
    XOR BX,BX
    XOR DX,DX

;on itère 216-1 fois
:boucle
    ADD DX,BX
    ADC BX,AX
    ADC AX,0000
LOOP boucle

;encore un tour
    ADD DX,BX
    ADC BX,AX
    
```

;sortie du résultat final

```

mov [BP]C2,DX
mov [BP]C1,BX
mov [BP]C0,AX

```

qui intègre l'équation (3) en nombres entiers avec  $\omega = 2^{16}$  en exécutant  $2^{16}$  itérations; ce qui revient, classiquement, à l'intégrer sur  $[0,1]$  en prenant un pas de  $2^{-16}$ .

Temps d'exécution sur AT 10 mhz: 0.12 s

Les calculs sont effectués à l'intérieur du processeur. Bien que seule la dernière valeur soit extraite du processeur vers la mémoire il ne serait pas difficile de faire de même à chaque itération ou après un nombre prédéfini de boucles. Signalons que si tous les résultats intermédiaires sont exportés vers la mémoire le temps d'exécution de cet algorithme est de 0.25 s.

#### 4 L'algorithme d'Euler modifié en nombres entiers.

Numérisons maintenant la méthode d'Euler modifiée, d'ordre 2 et constatons les différences avec la première méthode.

La discrétisation de la solution  $y$  de (1) vérifiant  $y(0)=1$  étant désignée par par  $Y_n = y(n/\omega)$ , la méthode d'Euler modifiée consiste à évaluer

$$Y_{n+1} = Y_n + \frac{Y_n}{\omega}$$

que l'on considère comme valeur intermédiaire et

$$Y_{n+2} = Y_n + \frac{2Y_{n+1}}{\omega} = Y_n + \frac{2Y_n}{\omega} + \frac{2Y_n}{\omega^2} \quad (4)$$

que l'on retient effectivement; avec cette indexation,  $N$  itérations de l'algorithme (4) correspondent, à  $2N$  itérations de l'algorithme d'Euler précédent. Nous pouvons projeter (4) dans la base de numération  $\omega$  en associant à  $Y_n$  un rationnel

$$Y_n = C_0 + \frac{C_1}{\omega} + \frac{C_2}{\omega^2} + \frac{C_3}{\omega^3} \quad (5)$$

où les  $c_i \in [0, \omega-1]$  et à  $Y_{n+1}$  un terme analogue

$$Y_{n+1} = \bar{C}_0 + \frac{\bar{C}_1}{\omega} + \frac{\bar{C}_2}{\omega^2} + \frac{\bar{C}_3}{\omega^3}$$

en déterminant les retenues induites. Reportons (5) dans (4), nous obtenons, en ne retenant que quatre chiffres, la relation

$$Y_{n+2} = C_0 + \frac{C_1}{\omega} + \frac{2C_0}{\omega} + \frac{C_2}{\omega^2} + \frac{2C_1}{\omega^2} + \frac{2C_0}{\omega^2} + \frac{C_3}{\omega^3} + \frac{2C_2}{\omega^3} + \frac{2C_1}{\omega^3}$$

puis les récurrences suivantes exprimant les chiffres de  $Y_{n+2}$  à l'aide de ceux de  $Y_n$ :

#### Algorithme 2

$$\begin{aligned} \bar{c}_3 &= \{c_3 + 2c_2 + 2c_1\} \\ \bar{c}_2 &= \{c_2 + 2c_1 + 2c_0 + [c_3 + 2c_2 + 2c_1]\} \\ \bar{c}_1 &= \{c_1 + 2c_0 + [c_2 + 2c_1 + 2c_0 + [c_3 + 2c_2 + 2c_1]]\} \\ \bar{c}_0 &= c_0 + [c_1 + 2c_0 + [c_2 + 2c_1 + 2c_0 + [c_3 + 2c_2 + 2c_1]]] \end{aligned} \tag{6}$$

Cet algorithme que nous venons d'établir rassemble en une seule étape les calculs réclamés par la méthode d'Euler modifiée pour l'intégration de l'équation différentielle (1). L'indexation utilisée montre qu'il suffit, pour intégrer l'équation de a à b, d'appliquer  $[(b-a)/2]$  fois l'algorithme à partir de la valeur initiale déterminée par l'expression de  $\exp(a)$  en base  $\omega$ . Si  $a=1$  et  $\omega=100$  nous pouvons prendre pour valeurs initiales  $c_0=2$ ,  $c_1=71$ ,  $c_2=82$ ,  $c_3=81$ .

#### Résultats numériques

Si  $\omega=10000$ ,  $a=0$ ,  $b=10000$ , l'algorithme nous permet de construire 5000 points d'une approximation discrète à 8 chiffres significatifs de la fonction exponentielle sur l'intervalle unité.

Le temps d'exécution est de 0.20s sur un AT 10mhz.

L'ordre de la méthode est 2: le nombre de chiffres significatifs est le double du nombre de chiffres significatifs de  $\omega-1$ . Nous rassemblons dans un tableau quelques valeurs de  $\omega$  et de l'approximation de e obtenue en intégrant sur  $[0, \omega/2]$  par l'algorithme 2.

$\omega$	e
10	2.7
100	2.718
1000	2.71828
10000	2.7182818

figure 2

En comparant avec les résultats de l'algorithme précédent nous voyons bien le gain obtenu par cette nouvelle version.

##### 5 Implémentation de l'Algorithme 2 en langage machine.

La version numérisée de l'algorithme d'Euler modifié est, elle aussi, parfaitement adaptée à une implantation processeur. En prenant pour base  $\omega = 2^{16}$ , une intégration de  $y'=y$  sur  $[0, 1]$  via  $2^{15}$  itérations de (6), peut être conduite en 0.6 s à 10 mhz. Au cours du calcul la précision des résultats est constamment supérieure à 10 chiffres significatifs. Voici l'adaptation en langage machine 8086 de (6) permettant d'obtenir ces valeurs:

```
MOV CX,[BP+c0]
MOV DX,[BP+c1]
MOV SI,[BP+c2]
MOV DI,[BP+c3]
```

```
MOV AX,DI
XOR BX,BX
```

```
ADD AX,SI
ADC BX,+00
ADD AX,SI
ADC BX,+00
ADD AX,DX
ADC BX,+00
ADD AX,DX
ADC BX,+00
MOV [BP+c3],AX
```

```
MOV AX,BX
XOR BX,BX
```

```
ADD AX,SI
ADC BX,+00
ADD AX,DX
ADC BX,+00
ADD AX,DX
ADC BX,+00
ADD AX,CX
ADC BX,+00
ADD AX,CX
ADC BX,+00
MOV [BP+c2],AX
```

```
MOV AX,BX
XOR BX,BX
```

```
ADD AX,DX
ADC BX,+00
ADD AX,CX
ADC BX,+00
```

```

ADD AX,CX
ADC BX,+00
MOV [BP+c1],AX
ADD BX,CX
MOV [BP+c0],BX

```

Après l'initialisation de  $c_3$ ,  $c_2$ ,  $c_1$  et  $c_0$  avec les chiffres de  $\exp(i/\omega)$ , l'exécution de ces instructions replace dans ces variables les chiffres de l'expression de  $\exp((i+2)/\omega)$  en base  $\omega$ . En les répétant autant que nécessaire nous pouvons, comme indiqué, intégrer très rapidement l'équation  $y' = y$  sur un intervalle quelconque de  $\mathbb{R}$ .

Dans la figure 3 suivante nous avons rassemblé les éléments, temps de calcul (en secondes), précision (nombre de chiffres significatifs à l'arrivée le dernier résultat devant être e), permettant d'évaluer notre approche.

Algorithme	ordre	$\omega$	nb iter	précision	temps
1	1	10000	10000	4	0,10
1	1	$2^{16}$	$2^{16}$	5	0,25
2	2	10000	5000	8	0,20
2	2	$2^{16}$	$2^{15}$	10	0,60

figure 3

Les exécutions ont été effectuées sur un compatible AT 10mhz. D'autres algorithmes ont été également traités dans la base  $\omega = 2^{16}$  en langage machine. Une version de l'algorithme d'Euler modifié détermine  $2^{15}$  valeurs de l'exponentielle, chacun avec 10 chiffres significatifs, en 600 ms (10mhz).

Nous abordons, dans les derniers paragraphes, le traitement en nombres entiers de diverses fonctions élémentaires; Nous ne rentrons plus dans la question de la traduction des algorithmes obtenus dans un langage de programmation ni dans les résultats concernant les temps d'exécution. Disons simplement que cette approche conduit à des programmes généralement saisissants.

## 6 Logarithme et nombres entiers

Etudions à présent l'analogie en nombres entiers du logarithme. Définissons le à partir de l'équation aux différences finies

$$u_{i+1} - u_i = \omega^2/i \quad (1)$$

traduction discrète de l'équation différentielle ordinaire  $u' = 1/x$ .

Posons  $u_i = x_i \omega + y_i$ , l'équation (1) devient

$$x_{i+1} \omega + y_{i+1} = x_i \omega + y_i + \omega^2/i \quad (2)$$

d'où nous déduisons immédiatement l'algorithme

$$\begin{aligned} x_{i+1} &= x_i + [(y_i + [\omega^2/i])/\omega] \\ y_{i+1} &= \{(y_i + [\omega^2/i])/\omega\} \end{aligned}$$

Cet algorithme, d'une grande simplicité, donne de très bons résultats pratiques.

## 7 La fonction $\sqrt{x}$ en nombres entiers.

Donnons un algorithme de tracé de la fonction  $\sqrt{ax}$  où  $a$  est un paramètre, à partir de l'équation différentielle

$$2 y y' = a$$

ou, en changeant la constante

$$y y' = a \quad (1)$$

Comme dans notre premier exemple posons  $y' = \frac{y_{n+1} - y_n}{1/\omega}$ , l'équation devenant

$$y_{n+1} = y_n + \frac{a}{\omega y_n} \quad (2)$$

Afin de traiter directement les retenues introduisons le développement en base  $\omega$  de  $y_n = u_n + \frac{v_n}{\omega}$  où  $u_n$  et  $v_n$  sont des entiers strictement inférieurs à  $\omega$ . Reportons dans (2), après une approximation évidente nous obtenons l'équation

$$y_{n+1} = u_n + \frac{u_n v_n + a}{\omega u_n}$$

d'où les relations de récurrence entre nombres entiers

$$\begin{aligned} u_{n+1} &= u_n + \left[ \frac{u_n v_n + a}{\omega u_n} \right] \\ v_{n+1} &= \left\{ \frac{u_n v_n + a}{\omega u_n} \right\} \end{aligned}$$

L'implémentation en langage de programmation de haut niveau, ou en langage machine ne pose pas de difficulté.

## 8 Coniques.

Traitons le cas du cercle d'abord. Il sera obtenu, dans un premier temps, à partir de l'équation  $y = \sqrt{b - ex^2}$  solution de l'équation différentielle  $y y'$

= -ex

Le même procédé que ci-dessus donne d'abord l'équation aux différences finies

$$y_{n+1} = y_n - \frac{en}{y_n}$$

dans laquelle nous remplaçons  $y_n$  par son expression  $y_n = u_n + \frac{v_n}{\omega}$  où  $u_n$  et  $v_n$  sont deux entiers inférieurs à  $\omega$ ; il vient très facilement les relations suivantes

$$u_{n+1} = u_n + \left[ v_n - \left[ \frac{ne\omega}{fu_n} \right] \right]$$

$$v_{n+1} = \left\{ v_n - \left[ \frac{ne\omega}{fu_n} \right] \right\}$$

dans lesquelles la constante d'excentricité  $e$  a été remplacée par  $e/f$ ,  $e$  et  $f$  entiers, pour permettre une plus grande souplesse dans l'approximation.

### 9 Cercles discrets.

Les systèmes différentiels peuvent également être traités par notre méthode ce qui fournira un deuxième algorithme pour la discrétisation du cercle; les solutions du système différentiel

$$x' = y$$

$$y' = -x$$

sont les cercles centrés à l'origine; appliquons notre méthode. Deux équations aux différences

$$x_{n+1} = x_n + \frac{y_n}{\omega}$$

$$y_{n+1} = y_n - \frac{x_n}{\omega}$$

sont naturellement associées au système; posons ensuite

$$x_n = u_n + \frac{\delta u_n}{\omega}$$

$$y_n = v_n + \frac{\delta v_n}{\omega}$$

où  $u_n, v_n, \delta u_n, \delta v_n$  sont des entiers  $< \omega$ .

Le même traitement que ci-dessus donne les relations de récurrence entre ces entiers

$$u_{n+1} = u_n + \left[ \frac{\delta u_n + v_n}{\omega} \right]$$

$$\begin{aligned}\delta u_{n+1} &= \left\{ \frac{\delta u_n + v_n}{\omega} \right\} \\ v_{n+1} &= v_n + \left[ \frac{\delta v_n - u_n}{\omega} \right] \\ \delta v_{n+1} &= \left\{ \frac{\delta v_n - u_n}{\omega} \right\}\end{aligned}$$

Pour obtenir toutes les coniques par procédé unique nous pouvons partir du système

$$x' = ay$$

$$y' = bx$$

conduisant aux récurrences entières suivantes:

$$\begin{aligned}u_{n+1} &= u_n + \left[ \frac{\delta u_n + av_n}{\omega} \right] \\ \delta u_{n+1} &= \left\{ \frac{\delta u_n + av_n}{\omega} \right\} \\ v_{n+1} &= v_n + \left[ \frac{\delta v_n + bu_n}{\omega} \right] \\ \delta v_{n+1} &= \left\{ \frac{\delta v_n + bu_n}{\omega} \right\}\end{aligned}$$

avec lesquelles  $a > 0$ ,  $b < 0$  donne les ellipses, (prendre  $b = -a$  pour les cercles) et  $a < 0$ ,  $b < 0$  les hyperboles.

#### 10 L'équation du pendule forcé.

Abordons l'équation vérifiée par les trajectoires d'un pendule forcé

$$x'' = a \sin x + b \cos t \quad (1)$$

que nous étudierons à travers le système différentiel

$$\begin{aligned}x' &= y \\ y' &= a \sin x + b \cos t\end{aligned} \quad (2)$$

Discretisons (2) par une méthode usuelle:

$$\begin{aligned}X_{n+1} &= X_n + \frac{Y_n}{\omega} \\ Y_{n+1} &= Y_n + a \frac{\sin X_n}{\omega} + \frac{\cos n}{\omega}\end{aligned} \quad (3)$$

Associations comme nous l'avons fait depuis le début du chapitre des entiers écrits en base  $\omega$  aux diverses grandeurs qui interviennent. Remarquons ici que  $X_n$  et  $Y_n$  ne sont pas les seules grandeurs à traiter, il faut aussi projeter  $\sin X_n$  et  $\cos n$  dans la base  $\omega$ ; mais alors, vu notre approche il faut simultanément évaluer  $\cos X_n$  et  $\sin n$ . D'où les choix de rationnels suivants

$$X_n = x_0 + \frac{x_1}{\omega} + \frac{x_2}{\omega^2}$$

$$Y_n = y_0 + \frac{y_1}{\omega} + \frac{y_2}{\omega^2}$$

$$C_n = c_0 + \frac{c_1}{\omega} + \frac{c_2}{\omega^2}$$

$$S_n = s_0 + \frac{s_1}{\omega} + \frac{s_2}{\omega^2}$$

$$U_n = u_0 + \frac{u_1}{\omega} + \frac{u_2}{\omega^2}$$

$$V_n = v_0 + \frac{v_1}{\omega} + \frac{v_2}{\omega^2}$$

respectivement associés aux valeurs  $X_n$ ,  $Y_n$ ,  $\cos n$ ,  $\sin n$ ,  $\cos X_n$  et  $\sin X_n$ .

Etant analogues aux exemples déjà vus les reports de retenues concernant  $X_n$ ,  $Y_n$ ,  $C_n$  et  $S_n$  ne posent pas de difficulté, détaillons ceux associés aux chiffres de  $U_n$  et  $V_n$ .

Partons des relations suivantes:

$$\cos X_{n+1} = \cos X_n - \frac{Y_n \sin X_n}{\omega^2}$$

$$\sin X_{n+1} = \sin X_n + \frac{Y_n \cos X_n}{\omega^2}$$

en effectuant séparément les produits des représentants de  $Y_n \sin X_n$  et  $Y_n \cos X_n$  dans lesquels nous ne conservons que les trois premiers termes, nous déterminons ceux de  $\cos X_{n+1}$  et  $\sin X_{n+1}$ :

$$\cos X_{n+1} = u_0 + \frac{u_1 - v_0 y_0}{\omega} + \frac{u_2 - v_0 y_1 - v_1 y_0}{\omega^2}$$

$$\sin X_{n+1} = v_0 + \frac{v_1 + u_0 y_0}{\omega} + \frac{v_2 + u_0 y_1 + u_1 y_0}{\omega^2}$$

Donnons directement les relations analogues liant les  $X_{n+1}$ ,  $Y_{n+1}$ ,  $C_{n+1}$ ,  $S_{n+1}$  et les chiffres des  $X_n$ ,  $Y_n$ ,  $C_n$  et  $S_n$ :

$$X_{n+1} = x_0 + \frac{x_1 + y_0}{\omega} + \frac{x_2 + y_1}{\omega^2}$$

$$Y_{n+1} = y_0 + \frac{y_1 + av_0}{\omega} + \frac{y_2 + av_1}{\omega^2}$$

$$C_{n+1} = c_0 + \frac{c_1 - s_0}{\omega} + \frac{c_2 - s_1}{\omega^2}$$

$$S_{n+1} = s_0 + \frac{s_1 + c_0}{\omega} + \frac{s_2 + c_1}{\omega^2}$$

Nous pouvons maintenant traduire les reports de retenues et obtenir les chiffres des représentants de  $X_{n+1}$ ,  $Y_{n+1}$ ,  $C_{n+1}$ ,  $S_{n+1}$ ,  $U_{n+1}$  et  $V_{n+1}$  comme fonctions de ceux de  $X_n$ ,  $Y_n$ ,  $C_n$ ,  $S_n$ ,  $U_n$  et  $V_n$ .

La liste complète des récurrences est la suivante:

$$x_2 = \{x_2 + y_1\}$$

$$x_1 = \{x_1 + y_0 + [x_2 + y_1]\}$$

$$x_0 = x_0 + [x_1 + y_0 + [x_2 + y_1]]$$

$$y_2 = \{y_2 + av_1\}$$

$$y_1 = \{y_1 + av_0 + [y_2 + av_1]\}$$

$$y_0 = y_0 + [y_1 + av_0 + [y_2 + av_1]]$$

$$c_2 = \{c_2 - s_1\}$$

$$c_1 = \{c_1 - s_0 + [c_2 - s_1]\}$$

$$c_0 = c_0 + [c_1 - s_0 + [c_2 - s_1]]$$

$$s_2 = \{s_2 + c_1\}$$

$$s_1 = \{s_1 + c_0 + [s_2 + c_1]\}$$

$$s_0 = s_0 + [s_1 + c_0 + [s_2 + c_1]]$$

(4)

$$u_2 = \{u_2 - v_0 y_1 - v_1 y_0\}$$

$$u_1 = \{u_1 - v_0 y_0 + [u_2 - v_0 y_1 - v_1 y_0]\}$$

$$u_0 = u_0 + [u_1 - v_0 y_0 + [u_2 - v_0 y_1 - v_1 y_0]]$$

$$v_2 = \{v_2 + u_0 y_1 + u_1 y_0\}$$

$$v_1 = \{v_1 + u_0 y_0 + [v_2 + u_0 y_1 + u_1 y_0]\}$$

$$v_0 = v_0 + [v_1 + u_0 y_0 + [v_2 + u_0 y_1 + u_1 y_0]]$$

Les relations (4) constituent une conversion en Nombres Entiers de la méthode d'Euler appliquée à l'équation (1). Nous pouvons, grâce à elles, intégrer cette équation différentielle par le seul truchement d'un processeur ne connaissant que les opérations entières et accélérer notablement le tracé de ses solutions.

Une première version langage machine en 160 octets, où  $\omega$  est un entier quelconque, utilisant des divisions entières, permet d'évaluer 15000 termes successifs de cette suite en 1 seconde. Pour  $\omega$  égal à certaines puissances de 2 telles que  $2^8$ ,  $2^{16}$ ,  $2^{32}$ , il est possible en remplaçant les divisions par des décalages de multiplier par deux les performances précédentes. Signalons toutefois que la qualité numérique des résultats donnés par (4) ne permet qu'une étude qualitative de l'équation (1). Les méthodes d'ordre supérieur sont inévitables si nous voulons conduire une étude numérique de qualité.

Ces méthodes de simulation arithmétique du continu éclairent peut être un peu mieux cette partie inévitable du traitement numérique qui consiste à "exprimer" les nombres réels, objets intrinsèques, dans un système de numération. Les rapprochements, esquissés ici, avec l'arithmétique mériteraient certainement plus d'égards.

Les images obtenues par ordinateur des ensembles de Julia et de Mandelbrot ont, tout en popularisant ce sujet, donné envie aux mathématiciens de comprendre les structures qui y sont cachées et aux amateurs de les reproduire sur leurs écrans. Le contraste, inconnu il y a peu, entre leur complexité et la simplicité du système dynamique qui les engendre n'est certainement pas un élément négligeable dans cet intérêt. Mais l'enthousiasme du curieux retombe en général assez vite lorsqu'il découvre la quantité de calculs qu'elles cachent. Nous voudrions présenter ici quelques algorithmes rapides de génération des ensembles de Julia et de Mandelbrot propres à restituer ou à maintenir la spontanéité des relations entre la théorie et la représentation visuelle de ces systèmes dynamiques.

Notre approche consiste à simuler un coprocesseur arithmétique "logiciel" spécialisé pour le système dynamique quadratique  $z^2+c$ . Il est fondé sur un réexamen de la notion de nombre réel machine ou réel flottant et par son remplacement par une notion de virgule fixe formelle. Nous obtenons alors un système dynamique discret sur  $\mathbb{Z}^2$  tout à la fois capable de capter l'essentiel des structures des ensembles de Julia et de Mandelbrot et d'être itéré rapidement. Il est avantageux pour les utilisateurs de machines non munies de coprocesseurs et surtout pour les stations de travail dont les coprocesseurs ou cartes graphiques flottants sont très onéreux. Le rôle que nous faisons jouer aux nombres entiers laisse prévoir que l'accélération sera à son avantage sur des dispositifs les traitant efficacement comme c'est le cas sur des processeurs RISC. Nous présentons trois algorithmes dont seul le premier a fait l'objet d'une implémentation optimisée; les autres qui n'ont que récemment franchi le premier pas de l'évaluation semblent très prometteurs c'est ce qui nous autorise à les présenter ici.

Cet article n'est qu'un sous-produit d'un travail plus ambitieux visant, par l'emploi d'Analyse Non Standard, à arithmétiser l'Analyse et dont nous dirons quelques mots à la fin de cet exposé.

1 Le premier algorithme rapide: une famille de systèmes dynamiques quadratiques sur  $\mathbb{Z}^2$ .

Le système dynamique complexe associé à la transformation quadratique

$$z^2 + c \tag{1}$$

cache derrière la simplicité de sa définition une structure véritablement très compliquée. Les célèbres ensembles de Julia et de Mandelbrot qui expriment certains aspects de cette dynamique sont là pour témoigner de cette richesse.

Rappelons brièvement qu'à toute valeur complexe  $c$  est associé un ensemble de Julia  $J_c$  défini comme frontière de l'ensemble  $K_c$  des nombres complexes dont la dynamique reste bornée.  $J_c$  est aussi l'adhérence de l'ensemble des cycles répulsifs. L'ensemble de Mandelbrot du système dynamique (1) est l'ensemble des valeurs  $c \in \mathbb{C}$  telles que  $J_c$  soit connexe; (voir [7], [36], [37]).

Nous définissons une famille de systèmes dynamiques discrets dépendant d'un paramètre entier  $\omega$  qui, pour  $\omega$  fixé, donne une discrétisation de (1) et qui converge vers lui si le paramètre  $\omega$  devient grand. Chacun dépend d'une variable complexe et d'un paramètre complexe "arithmétisés"  $x+iy$  et  $a+bi$  et se comporte, si nous le regardons convenablement, c'est à dire "de loin", comme le système (1): il possède des analogues des ensembles de Julia et un ensemble de Mandelbrot.

L'arithmétisation des variables et paramètres se fait en associant à  $z = x+iy$  et  $c = a+ib$  leurs projections dans un système de numération de base quelconque  $\omega$  à deux chiffres pour  $x$  et  $y$ , et trois chiffres pour  $a$  et  $b$ . Ceci revient à introduire les expressions:

$$\begin{aligned} x &= x_0 + \frac{x_1}{\omega} \\ y &= y_0 + \frac{y_1}{\omega} \\ a &= a_0 + \frac{a_1}{\omega} + \frac{a_2}{\omega^2} \\ b &= b_0 + \frac{b_1}{\omega} + \frac{b_2}{\omega^2} \end{aligned} \tag{i}$$

où  $x_0, x_1, y_0, y_1, a_0, a_1, a_2, b_0, b_1, b_2$  sont des chiffres c'est à dire des entiers de l'intervalle  $[0, \omega-1]$ .

En évaluant  $z^2+c$  à l'aide des relations (i) nous obtenons

$$\begin{aligned} z^2+c &= x_0^2 - y_0^2 + a_0 + \frac{2(x_0 x_1 - y_0 y_1) + a_1}{\omega} + \frac{x_1^2 - y_1^2 + a_2}{\omega^2} \\ &+ i \left[ 2x_0 y_0 + b_0 + \frac{2(x_0 y_1 + y_0 x_1) + b_1}{\omega} + \frac{2x_1 y_1 + b_2}{\omega^2} \right] \end{aligned} \tag{ii}$$

La considération des ordres de grandeur des itérations à effectuer ainsi que le désir d'accélérer leur traitement conduisent à projeter l'évaluation de  $z^2+c$  dans la base de numération  $\omega$  sous la forme:

$$z^2+c = x'_0 + \frac{x'_1}{\omega} + i(y'_0 + \frac{y'_1}{\omega}) \tag{iii}$$

En particulier  $x'_0, x'_1, y'_0$  et  $y'_1$  doivent être des chiffres de la base c'est à dire éléments de l'intervalle  $[0, \omega-1]$ . En fait ceci n'est vraiment requis que pour  $x'_1$  et  $y'_1$  ce qui allège déjà les calculs. Sur l'expression (ii) nous

remarquons d'une part que les numérateurs ne sont pas a priori des chiffres de la base  $\omega$  et qu'il y a un chiffre de trop. Pour mettre (ii) sous la forme (iii) il faut donc à la fois gérer les retenues et faire une approximation. Les reports de retenues ne sont que les quotients de divisions entières par  $\omega$  et les chiffres définitifs sont les restes de ces divisions. Pour alléger un peu nos notations nous désignons respectivement par  $[x]$  et  $\{x\}$  le quotient et le reste de la division euclidienne de  $x$  par  $\omega$  autrement dit  $[x]$  désigne ce qui est traditionnellement noté  $\left[\frac{x}{\omega}\right]$  ou  $x \text{ div } \omega$  et  $\{x\}$  désigne  $\left\{\frac{x}{\omega}\right\}$  ou  $x \text{ mod } \omega$ . L'approximation que nous faisons consiste à ne retenir des troisièmes chiffres de (ii) que leurs reports de retenues et à négliger leurs restes ie à transférer respectivement  $\left[x_1^2 - y_1^2 + a_2\right]$  et  $\left[2x_1 y_1 + b_2\right]$  sur les termes en  $\frac{1}{\omega}$ . La gestion des retenues ainsi décrite permet d'exprimer les chiffres du résultat, ici  $z^2 + c$ , en fonction des chiffres des variables et paramètres et conduit aux relations de récurrence suivantes.

$$\begin{aligned}
 x'_1 &= \left\{ 2(x_0 x_1 - y_0 y_1) + a_1 + \left[ x_1^2 - y_1^2 + a_2 \right] \right\} \\
 x'_0 &= x_0^2 - y_0^2 + a_0 + \left[ 2(x_0 x_1 - y_0 y_1) + a_1 + \left[ x_1^2 - y_1^2 + a_2 \right] \right] \\
 y'_1 &= \left\{ 2(x_0 y_1 + y_0 x_1) + b_1 + \left[ 2x_1 y_1 + b_2 \right] \right\} \\
 y'_0 &= 2x_0 y_0 + b_0 + \left[ 2(x_0 y_1 + y_0 x_1) + b_1 + \left[ 2x_1 y_1 + b_2 \right] \right]
 \end{aligned} \tag{2}$$

Partant d'un point  $z = x_0 \frac{x_1}{\omega} + i(y_0 \frac{y_1}{\omega})$ , le paramètre  $c = a + ib$  étant fixé les relations précédentes permettent d'évaluer  $z^2 + c$  et d'itérer cette évaluation en n'effectuant que des calculs sur des entiers. Pour des raisons d'efficacité nous choisissons évidemment  $\omega$  de la forme  $2^n$  de façon à éviter le recours aux opérations div et mod. C'est notre premier algorithme rapide.

Nous trouvons commode de faire subir une homothétie de rapport  $\omega$  aux variables et paramètres introduits en (i) de façon à n'avoir à considérer que des points à coordonnées entières. Ceci revient à travailler sur  $Z^2$  après avoir fait le choix d'une "unité".

Nous avons choisi de représenter le paramètre  $c$  avec 3 chiffres; le dernier chiffre, dont les composantes réelles et imaginaire sont  $a_2$  et  $b_2$ , peut être supprimé si l'on ne veut pas contrôler trop finement la dépendance en  $c$  de (1). Il est bien sûr possible de traiter plus de chiffres pour  $z$  et  $c$ , généralisant les relations (2) à des multiprécisions quelconques. Ceci conduit à de nombreuses variantes; toutefois nos expérimentations ont montré que (2) est très efficace pour générer les images classiques attribuées au comportement de (1).

En fait l'examen du comportement de (2) en précision volontairement limitée (par exemple  $\omega=100$ ) montre des ressemblances indéniables avec ce que nous connaissons de (1). Il semble que notre système discret possède un grand nombre de propriétés mathématiques remarquables mais les troncatures qui apparaissent dans les récurrences arithmétiques (2) ne nous permettent malheureusement pas encore de décrire théoriquement son comportement. Insistons sur une propriété remarquable de ce système: bien que nous négligions, dans (2), les termes en  $\omega^{-2}$  nous tenons compte, comme nous l'avons dit, de leurs reports de retenue sur les termes en  $\omega^{-1}$ . Nous avons constaté que le comportement du système s'éloigne complètement de celui de (1) si nous négligeons ces retenues. En ce sens (2) est optimal.

La convergence en  $\omega$  vers (1) est claire puisque ce paramètre contrôle à la fois le degré d'approximation des variables et la précision des calculs.

## 2 Résultats pratiques.

Une implémentation très optimisée de cet algorithme avec  $\omega=2^{14}$  a été réalisée par J.M. Lecorché dans le but de produire des images d'ensembles de Julia et de Mandelbrot. Ce programme supporte un nombre variable de chiffres compris entre 1 et 4 ce qui équivaut à une précision flottante de 4, 8, 12 ou 14 chiffres décimaux. La dernière est donc proche de celle des réels flottants double précision du langage C. La souplesse et la structure de l'algorithme apportent un gain de temps très appréciable à la génération d'images de qualité telles que celles publiées dans [78]. Sur une machine sans coprocesseur, un SUN 4/110, nous avons observé une division du temps par un facteur  $> 60$  dans l'obtention d'une image de l'ensemble de Mandelbrot complet juste cadré sur un écran 1024x1024 (256 couleurs); l'algorithme entier utilisait 2 chiffres, la version classique utilisait les float du C. Sur une machine munie de coprocesseur comme un SUN 386 (20 Mhz) l'implémentation de (2) sur le processeur 386 de précision comparable aux réels flottants est légèrement plus rapide que la version flottante utilisant le 387. Mais même pour ce genre d'équipements les implémentations de précision inférieure se montrent très utiles soit pour générer des images d'ensembles de Julia complets ou légèrement agrandis qui ne réclament pas toute la précision de l'arithmétique flottante soit pour faire du prototypage rapide dans une zone en cours d'exploration; le temps d'exécution pouvant être divisé par un facteur 4 ou 5.

Donnons quelques temps d'exécutions obtenus sur ces machines.

SUN386	Re x	Im x	Re c	Im c	préc.	iter	temps (s)
	-1.5...1.5	-1.5...1.5	0.00000	1.00000	2	256	134
	-1.7...1.7	-1.7...1.7	-0.15652	1.03225	2	256	167
	-1.8...1.8	-1.8...1.8	-1.25000	0.00000	2	256	619
	-1.4...1.4	-1.4...1.4	-0.12000	0.74000	2	256	2050
	-1.3...1.3	-1.3...1.3	0.27334	0.00742	2	256	3443

Temps d'exécution pour ensembles de Julia (1024x1024)  
par l'algorithme en nombres entiers sur processeur 386

SUN387	Re x	Im x	Re c	Im c	préc.	iter	temps (s)
	-1.5...1.5	-1.5...1.5	0.00000	1.00000	2	256	169
	-1.7...1.7	-1.7...1.7	-0.15652	1.03225	2	256	203
	-1.8...1.8	-1.8...1.8	-1.25000	0.00000	2	256	742
	-1.4...1.4	-1.4...1.4	-0.12000	0.74000	2	256	2224
	-1.3...1.3	-1.3...1.3	0.27334	0.00742	2	256	4062

Temps d'exécution pour ensembles de Julia (1024x1024)  
par l'algorithme réel classique sur coprocesseur 387

Où nous constatons que l'algorithme (2) exécuté en nombres entiers sur un processeur entier rattrape son homologue flottant exécuté sur un coprocesseur. Des mesures analogues sur SUN4 non équipé de coprocesseur donnent une division du temps d'exécution par un facteur d'environ 60. Ceci est en accord avec les facteurs d'accélération des coprocesseurs que les constructeurs estiment généralement autour d'un facteur 50. Voici quelques résultats obtenus sur SUN4 architecture RISC en simple précision.

SUN4	Re x	Im x	Re c	Im c	préc.	iter	temps (s)
	-1.5...1.5	-1.5...1.5	0.00000	1.00000	1	256	58
	-1.7...1.7	-1.7...1.7	-0.15652	1.03225	1	256	71
	-1.8...1.8	-1.8...1.8	-1.25000	0.00000	1	256	262
	-1.4...1.4	-1.4...1.4	-0.12000	0.74000	1	256	887
	-1.3...1.3	-1.3...1.3	0.27334	0.00742	1	256	1327

Temps d'exécution pour ensembles de Julia (1024x1024)  
par l'algorithme en nombres entiers

SUN4	Re x	Im x	préc.	iter	temps (s)
	-2.00...0.50	-1.25...1.25	1	256	1222
	-0.95...-0.88	0.23...0.29	1	256	1382
	-2.00...0.50	-1.25...1.25	1	2048	8828
	-2.00...0.50	-1.25...1.25	2	256	3672
	-2.00...0.50	-1.25...1.25	2	2048	28100

Temps d'exécution pour ensemble de Mandelbrot (1024x1024)  
par l'algorithme en nombres entiers

Les mesures de différences point par point des images obtenues montrent l'avantage apporté par la possibilité de travailler en précision réduite avec l'algorithme (2).

### 3 Les discrétisations provoquées par l'ordinateur.

Les images maintenant bien connues des systèmes dynamiques quadratiques sont en fait celles des systèmes discrets que l'ordinateur introduit implicitement. Commençons par analyser, pour en tirer parti dans les deux algorithmes suivants, ces discrétisations que le traitement sur machine fait subir à tout calcul "réel".

Deux aspects numérique et géométrique interviennent. Le premier n'est présent que dans les ordinateurs non munis de coprocesseurs: la compilation convertit tous les calculs flottants en opérations arithmétiques. C'est une discrétisation numérique ou arithmétique visible sur le code machine fourni par le compilateur.

Le deuxième résulte de la finitude des nombres réels disponibles dans une "arithmétique flottante" provoquant une discrétisation de fait de  $\mathbb{R}$ ,  $\mathbb{R}^2$  et plus généralement de tout objet continu. En particulier, ce traitement remplace le système dynamique complexe associé à la famille  $z^2+c$  par un système discret défini sur un sous-ensemble fini de  $\mathbb{R}^2$ .

Ces deux discrétisations sont bien entendu liées. Nous pourrions être tentés d'étudier ces discrétisations de notre système dynamique pour en tirer quelques améliorations ou optimisations mais il apparaît assez vite que la complexité du code machine d'une part ou la structure de l'ensemble des réels flottants d'autre part ne sont pas directement maniables. Nous avons préféré définir les systèmes dynamiques sur  $\mathbb{Z}^2$ , vus en (2), par une approche qui capte l'essentiel des deux aspects arithmétique et géométrique précédents et qui tout en donnant des résultats numériques similaires soit radicalement plus simple.

#### 4 Quelques faiblesses de l'arithmétique flottante.

Le gain de vitesse acquis par (2) n'étant pas dû à des notions de complexité d'algorithme nous en avons cherché, sans pour autant nous lancer dans une étude exhaustive des détails, une explication plausible. L'arithmétique flottante commode et indispensable dans bien des cas, possède quelques faiblesses bien connues.

Lorsque beaucoup d'itérations d'un calcul sont nécessaires pour aboutir à un résultat intéressant sans que les étapes précédentes ne présentent d'intérêt le calcul en nombres réels nécessite d'incessants transferts entre les registres du processeur et la mémoire. Ces échanges ralentissent beaucoup le déroulement des opérations. Une version entière "équivalente" de l'algorithme réel, permettant loger et maintenir la plus grande partie possible du calcul dans les registres, est toujours très avantageuse. A côté de cet avantage évident, des applications de notre méthode à d'autres situations ont aussi révélé les points sensibles suivants.

Dans les processeurs les plus répandus la gestion des retenues se fait au travers du bit de retenue; mais la propagation de cette information s'effectue au travers du canal de communication le plus étroit possible: 1 bit. Là aussi nous préférons gérer les reports de retenue via des canaux de taille plus conséquente, c'est à dire des registres ou des variables mémoire selon les circonstances.

Une image d'ensemble de Julia discrétisé comprenant un nombre fini de points ne nécessite pas toujours toute la précision de l'arithmétique flottante disponible; autrement dit dans un sous-espace  $X$  de  $\mathbb{R}^2$  la quantité d'information contenue dans l'assertion  $x \in X$  n'est pas indépendante de la position de  $x$  dans l'espace  $X$ . La rigidité de la virgule flottante ne permet pas de retirer de cette observation une économie effective dans la puissance de calcul; il n'y a pas d'autre recours que de la court-circuiter. Par ailleurs le calcul d'une expression peut nécessiter plus de précision à un endroit et moins ailleurs; là aussi l'arithmétique flottante manque de souplesse.

Les réels machine possèdent une certaine cohérence; si à un moment quelconque nous interrompons un processus numérique nous pouvons lire les développements décimaux de chaque variable utilisée. C'est un luxe qui se paie aussi en temps de calcul et que nous ne nous offrons plus en "éclatant" chaque nombre en une collection d'entiers indépendants: nous libérons les chiffres. C'est le coeur de la méthode qui nous permet d'utiliser au mieux la puissance de calcul d'un processeur et que nous nous permettons de présenter au lecteur même si elle nous éloigne quelques instants de la dynamique; elle lui servira peut-être dans d'autres occasions.

5 Une généralisation de cette approche: le Calcul en nombres entiers.

Cette méthode, que nous qualifions de Calcul en nombres entiers, est une généralisation du petit calcul qui nous a conduit à la relation (2). Ce Calcul améliore souvent de façon notable les inconvénients des réels flottants entraînant d'appréciables gains dans les temps de calculs. De plus, même s'il n'est pas encore possible dans chaque application de prévoir ces gains, les perspectives théoriques qu'ouvre cette méthode sont toujours instructives. En effet, comme pour les équations aux différences finies, elle est à la fois un moyen effectif de calcul numérique et un outil théorique convertissant les notions réelles en notions arithmétiques. Le Calcul en nombres entiers est un traitement formel des chiffres intervenant dans une expression numérique ou un algorithme. Ce traitement comprend la gestion des retenues. Il pourrait également être qualifié de "projection" dans une base de numération. Il repose sur une discrétisation régulière de la droite réelle associée à un système de numération positionnelle en base  $\omega$ , entier donné, que nous décrivons.

Considérons l'ensemble  $\mathcal{D}_k$  des rationnels qui s'écrivent sous la forme

$$x = x_0 + \frac{x_1}{\omega} + \frac{x_2}{\omega^2} + \dots + \frac{x_k}{\omega^k}$$

où  $x_0$  est un entier et  $x_1, x_2, \dots, x_k$  sont des chiffres en base  $\omega$ , ie des entiers de l'intervalle  $[0, \omega-1]$ ; ce sont les développements en base  $\omega$  de longueur  $k+1$ . Nous pouvons introduire des nombres complexes de ce type et généraliser les opérations usuelles de façon canonique. Il est courant d'avoir à évaluer des expressions portant sur des réels. Nous obtiendrons des résultats analogues au calcul classique si nous parvenons à exprimer les chiffres du résultat d'un calcul en fonction des chiffres des données ou des variables. Ceci est possible dans de nombreuses situations. Lorsque c'est le cas nous obtenons des algorithmes d'évaluation très efficaces; les remarques précédentes s'appliquent mais une autre également: l'algorithme induit sur les chiffres est une sorte de prétraitement formel fait une fois pour toute. La seule difficulté réside dans la gestion des retenues. Mais ici ce n'est pas une tache insurmontable et nous aurions tort de nous priver de certains avantages gratuits qui en résultent. Nous simulons ainsi la somme et le produit d'une virgule fixe d'ordinateur.

Somme de deux éléments de  $\mathcal{D}_k$ .

Si  $x = x_0 + \frac{x_1}{\omega} + \frac{x_2}{\omega^2} + \dots + \frac{x_k}{\omega^k}$  et  $y = y_0 + \frac{y_1}{\omega} + \frac{y_2}{\omega^2} + \dots + \frac{y_k}{\omega^k}$  sont deux éléments de  $\mathcal{D}_k$  la somme

$$x+y = x_0+y_0 + \frac{x_1+y_1}{\omega} + \frac{x_2+y_2}{\omega^2} + \dots + \frac{x_k+y_k}{\omega^k}$$

n'est pas en général dans  $\mathcal{D}_k$ ; nous la mettons sous la forme requise en reportant les retenues. Pour cela nous introduisons les notations suivantes:  $[x]$  désignera le quotient entier (division euclidienne) de  $x$  par  $\omega$  et  $\{x\}$  le reste de la division de  $x$  par  $\omega$ . Alors

$$\begin{aligned}
 x+y = & x_0 y_0 + [x_1 y_1 + [x_2 y_2 + \dots + [x_k y_k ] \dots]] \\
 & + \frac{\{x_1 y_1 + [x_2 y_2 + \dots + [x_k y_k ] \dots]\}}{\omega} \\
 & + \frac{\{x_2 y_2 + [x_3 y_3 + \dots + [x_k y_k ] \dots]\}}{\omega^2} \\
 & + \dots + \frac{\{x_k y_k\}}{\omega^k}
 \end{aligned}$$

est mis sous forme d'un élément de  $\mathcal{D}_k$ . Des relations analogues peuvent être établies pour la soustraction.

#### Produit de deux éléments de $\mathcal{D}_k$

Le même principe s'adapte à la multiplication. Pour cette dernière nous avons

$$\begin{aligned}
 x.y = & x_0 y_0 + [x_0 y_1 + x_1 y_0 + \dots + [x_0 y_k + x_1 y_{k-1} + \dots + x_k y_0]] \\
 & + \frac{\{x_0 y_1 + x_1 y_0 + \dots + [x_0 y_k + x_1 y_{k-1} + \dots + x_k y_0]\}}{\omega} \\
 & + \frac{\{x_0 y_2 + x_1 y_1 + x_2 y_0 + \dots + [x_0 y_k + x_1 y_{k-1} + \dots + x_k y_0]\}}{\omega^2} \\
 & + \dots
 \end{aligned}$$

Contrairement aux apparences ces expressions se calculent très bien en cascade et condensent un grand nombre de retenues du processeur. Elles peuvent être logées dans des registres ou des variables assez grandes et condensent un grand nombre d'instructions et de manipulations du processeur dévolues la gestion du bit de retenue. Nous n'abordons pas ici l'algorithme de division plus délicat.

Si nous conservons les  $k+1$  premiers termes, ie les coefficients de  $\omega^{-1}$  pour  $1 \leq \omega \leq k$ , dans la formule précédente nous obtenons une approximation du produit comparable à celle d'une arithmétique à virgule fixe à multiprécision. Cette précision dépend de la taille de  $\omega$  et de  $k$ ; si par exemple  $\omega=1000$  et  $k=4$  la précision est de l'ordre d'une arithmétique à 12 chiffres décimaux.

De nombreuses applications de ce Calcul en nombres entiers ont été conduites à Strasbourg à la fois dans des domaines mathématiques et algorithmiques.

## 6 Un algorithme exploitant la dynamique.

L'avantage du système (2) que nous allons exploiter ici réside dans le fait qu'il est une discrétisation **explicite** de (1). De plus il est finitairement descriptible, c'est à dire qu'il ne contient qu'une quantité finie d'information, à priori entièrement accessible. Tout ce qui apparait sur les images des ensembles de Julia ou de Mandelbrot n'est qu'un transcodage, certe compliqué, des propriétés arithmétiques d'un nombre fini d'entiers. En effet l'essentiel du comportement de (2) est contenu dans des domaines bornés, donc finis, de  $\mathbb{Z}^2$  et leurs paramétrage est également décrit par des entiers. Notre système dynamique discret est un objet déterministe fini dont la complexité croît avec  $\omega$  et peut atteindre celle de son analogue continu (1).

Tout système discret fini possède une structure combinatoire canonique associée au graphe de sa transformation: son domaine se décompose en un nombre fini de bassins constitués d'arbres attachés à des cycles. Pour le système (2), défini sur  $\mathbb{Z}^2$ , il existe en plus un arbre attaché à l'infini. Ce graphe peut être exploité indépendamment de l'algorithme du §1 et permet de raccourcir encore les calculs; cette fois surtout pour des ensembles de Julia ou de Mandelbrot complets. L'idée consiste à le parcourir de la façon la plus économique possible ie sans repasser deux fois sur les mêmes points. Or c'est là que réside la plus grande perte de temps de l'algorithme classique: il peut provoquer de très longs parcours de ces cycles sans amélioration de la quantité d'information de l'image. Nous réalisons ces parcours économiques en implémentant en mémoire les sommets du graphe, c'est à dire les points du domaine de  $\mathbb{Z}^2$  étudié en nous laissant porter par la dynamique; il nous suffit de mémoriser notre passage à chaque sommet par une valeur que nous laissons tomber dans les cases mémoires correspondantes. L'algorithme est très simple; supposons que nous voulions analyser la dynamique d'un système discret contenu dans un carré de  $\mathbb{Z}^2$  formé de  $N \times N$  points. Nous supposons que ce domaine contient tous les bassins finis et une partie du bassin de l'infini (des variantes pour les "zooms" sont possibles). Nous initialisons une matrice  $M$  d'octets de taille  $N \times N$  avec des valeurs égales à  $-2$  par exemple dans laquelle nous obtenons à la fin une numérotation des bassins. Nous utilisons également une variable auxiliaire, initialement nulle, destinée à compter ces bassins. Le principe consiste à choisir les coefficients  $-2$  de cette matrice comme points de départ de trajectoires d'itération  $T$  au cours de laquelle nous associons la valeur  $-1$  aux coefficients rencontrés et à observer que ces

itérations conduisent obligatoirement à l'une des situations suivantes:

nous sortons de la matrice; notre point de départ appartient donc au bassin de l'infini; nous lui attribuons la valeur 0 ainsi qu'à tous ses itérés contenus dans M;

nous rencontrons un élément de M de valeur  $\geq 0$  ie nous rejoignons un bassin déjà rencontré; alors nous attribuons cette valeur au point de départ et à ses itérés contenus dans T.

nous rencontrons un élément de valeur  $-1$ , ie nous atteignons un nouveau cycle; alors nous augmentons d'une unité le nombre de bassins découverts et l'attribuons à T.

Il est clair qu'à la fin nous obtenons une numérotation des différents bassins de notre système dynamique, le bassin de l'infini étant numéroté 0. Remarquons qu'une modification évidente de cet algorithme, une variable supplémentaire, permet de déterminer la longueur des cycles ou la hauteur des arbres attachés. Il est alors commode de mémoriser toute cette information pour des traitements ultérieurs de la façon suivante. Supposons que nous sachions par ailleurs que l'arbre le plus haut à attacher ait une hauteur inférieure à 100; ceci implique que la distance itérative d'un noeud à son cycle limite est majorée par 100. Nous attribuons alors aux bassins des valeurs entières multiples de 100 ceci laissant de la place pour loger dans les intervalles ainsi définis les hauteurs des noeuds des arbres rencontrés. Par exemple le 3<sup>ième</sup> bassin rencontré portera la valeur 300 sur son cycle limite, la valeur 301 sur tous les points qui en une itération tombent sur ce cycle etc. Ce processus peut être évidemment automatisé; l'algorithme détecte alors lui-même le nombre d'itérations requises.

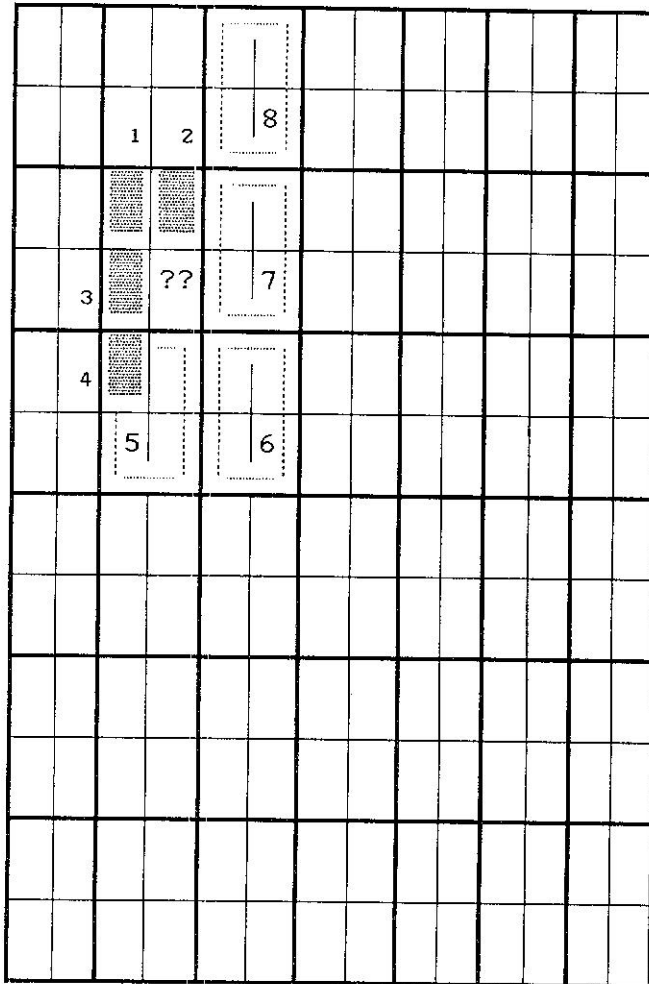
Cet algorithme dynamique n'a pas encore été codé avec le même niveau d'optimisation que le précédent; nous ne pouvons que donner l'ordre de grandeur provisoire, de l'ordre de 5, du facteur de réduction des temps de calculs par rapport à l'algorithme précédent. Nous rappelons que cet algorithme est surtout avantageux pour des dynamiques complètes; l'un de ses inconvénients, pour les micros-ordinateurs, est la taille mémoire requise (de l'ordre de 6 Mo pour des images 1024x1024).

## 7 L'algorithme dichotomique.

La facilité avec laquelle ces deux algorithmes nous ont fourni des images nous a conduit à faire quelques expériences naturelles. L'une d'elles consiste à superposer, pour une valeur complexe  $c$  fixée, l'ensemble de Julia donné par l'algorithme  $(Z_\omega)$  avec des gros pixels de taille  $2\tau$  et l'ensemble de Julia donné par l'algorithme  $(Z_{2\omega})$  avec des pixels de taille  $\tau$ . La bonne qualité de la superposition nous a donné l'idée de construire les images d'ensembles de

Julia ou de Mandelbrot par un procédé de raffinement le long des frontières des plages de niveaux des itérations. En effet nous voyons que les franges les plus éloignées des limites sont assez larges alors qu'elles se resserrent près de ces zones. Les points de ces franges les plus éloignés de leurs frontières contenant moins d'information devraient être plus facile à obtenir. Nous allons en tirer profit par un petit raisonnement topologique. Nous allons supposer que toute petite courbe fermée discrète dont la valeur d'échappement est constante est entièrement contenue dans une telle frange et qu'elle peut donc être remplie par les mêmes valeurs. L'algorithme est le suivant:

Nous initialisons une matrice de taille  $4N \times 4N$  où  $N$  est une puissance de 2 convenable avec la valeur 0 et déterminons l'ensemble de Julia  $J_2$  (ici  $\omega=2$ ) dans un espace dont les pixels ont une taille  $N \times N$ . Puis nous déterminons l'ensemble de Julia  $J_4$  et l'affichons avec des pixels de taille  $\frac{N}{2} \times \frac{N}{2}$ . Dans ce processus de subdivision nous ne traitons pas tous les pixels de taille  $\frac{N}{2} \times \frac{N}{2}$  et sautons tous les cas où le 8-voisinage mixte, décrit sur la figure suivante, a une valeur d'échappement constante.



L'algorithme dichotomique subdivise les pixels en 4 sous-pixels et ne lance une itération que pour les petits pixels dont la couronne mixte de ses 8 voisins représentée ici contient au moins deux couleurs distinctes.

Cet algorithme de dichotomie a été mis au point et implémenté pour évaluation par M.A. Jacob sur un SUN3/60 non équipé de coprocesseur; les images ont une résolution de 900x900. L'optimisation du code n'ayant pas encore été abordée il ne peut pas encore être comparé au premier algorithme. Nous le comparons à une version du premier algorithme d'optimisation équivalente et à la version flottante usuelle. Nous donnons ces résultats pour l'ensemble de Mandelbrot dans le tableau suivant où le petit carré du plan complexe examiné est défini par les coordonnées de son centre et par la longueur de son côté. Vu la longueur des calculs flottants nous n'avons pas encore généré toutes les images en réels flottants ce qui explique les lacunes de la colonne correspondante.

SUN3/60	centre x= y=	côté	réels (s)	algo1 (s)	algo3 (s)
	-0.5 0.0	3.0	18226	3475	550
	-0.59375 -0.65625	0.1875		3732	991
	0.71875 0.46875	0.1875		2977	880
	-0.15625 -1.03125	0.1875		1509	440
	-0.65625 0.46875	0.1875		7710	1470
	0.40625 -0.21875	0.1875	38307	12999	1232
	-0.12695 -0.99023	0.02734		971	437
	-0.17382 -1.07227	0.01171	6503	2209	687
	-0.10351 -0.94335	0.01171		3529	1431
	0.41601 -0.21289	0.01171		7612	3511
	0.39648 -0.27929	0.01171		3475	1245
	-0.66101 0.46667	0.00073		8331	3436
	-0.66076 0.46252	0.00073		11702	5549
	0.38928 -0.30505	0.00073		14646	11395
	0.38757 -0.31213	0.00073		14206	6700
	0.39245 -0.27453	0.00073	23680	12030	3796
	0.39465 -0.27746	0.00073		11599	3728
	-0.66069 0.46260	$4.5 \cdot 10^{-5}$		16478	8081
	0.38735 -0.31217	$4.5 \cdot 10^{-5}$	54347	29414	10088
	-0.66067 0.46262	$2.8 \cdot 10^{-6}$		19991	9612
	0.38733 0.31218	$2.8 \cdot 10^{-6}$	95634	25408	9183

Temps d'exécution d'aggrandissements de l'ensemble de Mandelbrot (900x900) sur SUN3/60 par algorithmes flottant, nombres entiers et dichotomique.

Nous constatons que l'algorithme dichotomique apporte encore un facteur de réduction très intéressant, autour de 3, par rapport à l'algorithme en nombres entiers. Même avec cette première évaluation imparfaite il semble tout à fait prometteur.

remarques.

La méthode employée permet de traiter plus soupement la coexistence de variables de précisions différentes dans un algorithme; ceci devrait se révéler utile aux traitements numériques des systèmes à forte sensibilité aux conditions initiales.

D'autres développements sont en cours, en particulier une parallélisation sur T-node.

Bien que les formules (2) permettent d'accélérer la génération des images les troncatures qui y figurent ne nous permettent pas encore de comprendre les structures qu'elles cachent; des travaux ultérieurs nous permettront, peut-être, d'y parvenir.

## BIBLIOGRAPHIE

- 1 ALBANO A. — Representation of Digitized Contours in Terms of Conic Arcs and Straight-Line Segments, *Computer Graphics and Image Processing*. 3, pp. 23-33, (1974).
- 2 ARABNIA H.R. et OLIVER M.A. — Arbitrary rotation of raster images with SIMD machine architectures. *Computer Graphics Forum* Vol 6, n° 1, Janvier 1987.
- 3 BAO P.G. et ROKNE J.G. — Quadruple-step Line Generation, *Computers and Graphics*, 13, (4), (1990).
- 4 BERNOULLI J. — Recueil pour les astronomes, Berlin, 1771.
- 5 BERSTEL J. — Tracé de droites, fractions continues et morphismes itérés. Colloque en l'honneur de Schutzenberger, pp 300-311, 1988.
- 6 BLANKINSHIP W.A. — A new version of the Euclidean algorithm, *Amer. Math. Monthly*, pp. 742-745, (1963).
- 7 BLANCHARD P. — Complex analytic dynamics on the Riemann sphere, *Bull. Amer. Math. Soc.* 11 n°1, pp 85-141, 1984.
- 8 BRACCINI C. et MARINO G. — Fast Geometrical Manipulations of Digital Images, *Computer Graphics and Image Processing* 13, pp 127-141 (1980).
- 9 BRAUER A. — On a problem of partitions, *Amer. J. Math.* 64 pp. 299-312 (1942).
- 10 BRESENHAM J. — Algorithm for computer control of a digital plotter, *IBM System Journal*, 1965, Vol 4, pp 25-30.
- 11 BRESENHAM J. — Ambiguities in incremental line rastering, *IEEE Computer Graphics and applications*, May 1987, pp 31-43.
- 12 BRONS R. — Linguistic methods for the description of a straight line on a grid, *Comp. Graph. Images Process.* 3, pp. 48-62, 1974.
- 13 BURN R.P. — A Pathway into Number Theory, Cambridge University Press, Cambridge, England (1982).
- 14 BURN R.P. — Groups, A Path to Geometry, Cambridge University Press, Cambridge, England, (1985).
- 15 CARTIER P. — Perturbations singulières des équations différentielles ordinaires et analyse non-standard, *Sém. Bourbaki* nov. 1981, *Astérisque* 92-93, pp. 21-44, (1982).
- 16 CARTIER P. — Sur une généralisation des symboles de Legendre-Jacobi, *Ens. Math.* t. 16, pp. 31-48, (1970).
- 17 CASTLE C.M.A. et PITTEWAY M.L.V. — An application of Euclid's algorithm to drawing straight lines, *NATO ASI Series, Vol F17, Fundamentals Algorithms for Computer Graphics*, R.A. Earnshaw Ed. Springer, 1985.

- 18 CESARO E. — Sur l'équation  $ax+by=n$ . Extraits d'une lettre à M. Hermite, Oeuvres complètes pp 283-293.
- 19 CHARDIN M. — Lien entre deux résultats sur la répartition modulo 1 de la suite des multiples d'un nombre réel, C.R.A.S. 308 pp. 519-520,(1989).
- 20 CHASSERY J.M. — Géométrie discrète: définitions et propriétés de base, Rapport de Recherche du RFMQ Laboratoire TIM3 IMAG Grenoble (1988).
- 21 CHASSERY J.M. et MONTANVERT A. — Géométrie Discrète, Hermès (1991).
- 22 CHRISTOFFEL E.B. — Observatio Arithmetica, Annali di Mathematica. 2nd series, Vol 6, 1875, pp 148-152.
- 23 CLAUSEN M. et FORTENBACHER A., —Efficient Solution of Linear Diophantine Equations, Preprint Univ. Karlsruhe, (1987).
- 24 COLIN de VERDIERE Y. — Nombre de points entiers dans une famille homothétique de domaines de  $\mathbb{R}^n$ , Ann. Sci. Ecole Norm. Sup. (4); 10 pp. 559-575, 1977.
- 25 COLLINS G.E. et LOOS R. —Polynomial Root Isolation by Differentiation, ACM Symposium on Symbolic and Algebraic Computation, pp. 15-25 (1976).
- 26 COUCHOT E. — Images, de l'optique au numérique, Hermès.
- 27 COVEN E.M. et HEDLUNG G.A. — Sequences with minimal block growth, Math. Syst. Th. 7, pp. 138-153, (1983).
- 28 CROFT G. — Unsolved problems in intuitive mathematics. Springer.
- 29 DAVENPORT H. — The Higher Arithmetic, An introduction to the Theory of Numbers, Fifth edition, Cambridge Univ. Press.
- 30 DELEST M. FEDOU J.M. — Introduction aux polyèdres en combinatoire d'après E. Ehrhart et R. Stanley — Rapport de recherche Uer de Mathématique et Informatique de l'Université de Bordeaux, (1989).
- 31 DIETER U. — Das Verhalten der Kleinschen Funktionen  $\log \sigma_{g,h}(\omega_1, \omega_2)$  gegenüber Modultransformationen und verallgemeinerte Dedekindsche Summen. Journ. Reine Angew. Math. 201, pp. 37-70, (1959).
- 32 DOBKIN D. et SILVER D.— Applied computational geometry. Toward robust solutions of basic problems, J. of Computer and System Sciences 40, pp 70-87, 1990.
- 33 DOIGNON J.P. — Convexity in crystallographical lattices, J. of Geometry 3, 1973, pp 71-85.
- 34 DORST L. et DUIN R.P.W. — Spirograph Theory: a framework for calculations on digitized straight lines, IEEE Trans. Pattern Anal. Mach. Intell. PAMI 6 (N°5), pp. 632-639, 1984.
- 35 DORST L. et SMEULDERS A.W.M. — Discrete representations of straight lines, IEEE Trans Pattern Anal. Mach. Intell. PAMI 6 (N°4) pp 450-463, 1984.

- 36 DOUADY A. — Systèmes dynamiques holomorphes, séminaire Bourbaki nov. 1982, Astérisque 105-106, (1983).
- 37 DOUADY A. et HUBBARD J.H. — Itération des polynômes complexes, cours 83-84, publications mathématiques d'Orsay.
- 38 DULUCQ S. et GOUYOU-BEAUCHAMP D. — Sur les facteurs des suites de Sturm, Rapport de Recherche de l'Université de Bordeaux, 1987.
- 39 EARNSHAW R.A. et PITTEWAY M.L.V. — Euclid's algorithm and line drawing, Fundamental algorithms in computer graphics, [R.A. Earnshaw Ed.], pp 101-106 Springer-Verlag Berlin 1985.
- 40 EHRHART E. — Polynômes arithmétiques et méthode des polyèdres en combinatoire, Int. series of num. Math., 35, Birkhäuser, Basel, 1977.
- 41 ERDÖS P., GRUBER P.M. et HAMMER J. — Lattice points, Pitman Mono. 39 (1989).
- 42 FICKEN F. — A. Rossers's Generalization of the Euclid Algorithm, Duke Math. J. 10, pp. 355-379, 1943.
- 43 FORREST A.R. — Fundamental algorithms for computer graphics, [R.A. Earnshaw Ed.], pp 707-724, Springer-Verlag Berlin 1985.
- 44 FRANCON J. — Topologie discrète et algorithmique graphique, Bigre+Globule n° 61-62, pp 91-96, Avril 1989.
- 45 FRANCON J. et REVEILLES J.P. — De l'imagerie digitale à la géométrie discrète, Colloque sur l'Imagerie, CTHS Avignon 1990 (à paraître).
- 46 FREEMAN H. — Boundary encoding and processing, Picture processing and Psychopictorics, [Lipkin et Rosenfeld Ed.], pp 241-266, Academic Press N.Y. 1970.
- FROBENIUS
- 47 GRAHAM R.L., KNUTH D.E. et PATASHNIK O. — Concrete mathematics, Addison-Wesley Reading Mass. (1989).
- 48 GREENE D.H. et YAO F.F. — Finite resolution Computational Geometry, Proceedings 27<sup>th</sup> IEEE Symp. on Found. Comp. Sci. Toronto pp 143-152.
- 49 GRUBER P.M. et LEKKERKERKER C.G. — Geometry of Numbers. North-Holland 1987.
- 50 GRUNBAUM B. et SHEPHARD G.C. — Tilings and patterns, Freeman, 1986.
- 51 HAMMER J. — Unsolved problems concerning lattice points, Research Notes in math 15, Pitman (1977).
- 52 HAMMER J. — Digital Convexity, Lecture given to the twelfth Australasian Conference on Combinatorial Mathematics, Perth, Manuscript, (1984).
- 53 HARDY G.H. et WRIGHT E.M. — An introduction to the theory of number, fifth edition, Oxford Sc. Pub., 1989.
- 54 HARDY G.H. — Ramanujan, Cambridge University Press, (1940).

- 55 HARTHONG J.— Eléments pour une théorie du continu, Astérisque 109/110 p 235, 1983.
- 56 HARTHONG J. —Le Moiré, *Advances in applied mathematics* 2, 24-75, (1981).
- 57 HELFRICH B. —Algorithms to Construct Minkowski Reduced and Hermite Reduced Lattice Bases, *Theoretical Computer Science* 41, pp. 125-139, 1985.
- 58 HERSCH R.D.— Raster rotation of bilevel bitmap images. *EuroGraphics 85* Elsevier Science Publishers, (1985).
- 59 HOBBY J.D. —Digitized Brush Trajectories, Report N° STAN-CS-85-1070, Dept. of Computer Science, Stanford University (1985).
- 60 HOBBY J.D. — Rasterizing Curves of Constant Width, *J.A.C.M.* Vol. 36, N° 2, Apr. 1989, pp. 209-229.
- 61 HUNG S.H.Y.— On the straightness of digital arcs, *IEEE Trans. on Pattern Analysis and Machine intelligence*, Vol PAMI-7 n°2, March 85, pp 203-215.
- 62 KIM C.E. — On the cellular convexity of complexes, *IEEE Trans. Pattern Analysis Mach. Intell.* PAMI-3, pp 617-625, (1981).
- 63 KIM C.E. — On cellular straight line segments, *Comp. Graph. Image Process.* 18, pp 369-381, 1982.
- 64 KIM C.E. et ROSENFELD A. — Digital straight lines and convexity of digital regions, *IEEE Trans. Pattern Anal. Mach. Intell.* PAMI 4, pp 149-153, 1982.
- 65 KIM C.E. et SLANSKY J. — Digital and cellular convexity, *Pattern Recognition* 15, pp. 359-367, (1982).
- 66 KNUTH D. — Notes on generalized Dedekind sums, *Acta Arithmetica*, XXXIII pp. 297-325, (1977).
- KO CHAO — Note on the lattice points in a parallelepiped, *J. Lond. Math. Soc.* 12, pp. 40-47, (1936).
- 67 KONG T.I. et ROSENFELD A.— Digital topology: Introduction and survey, *Computer vision, Graphics and Image processing* 48, pp 352-393, 1989.
- 68 KOPETZKY H.G. et SCHNITZER F.J. — A Geometrical Approach to Approximations by Continued Fractions, *J. Austral. Math. Soc (series A)* 43, pp. 176-186, 1987.
- 69 LEE H.C. et FU K.S. — Using the FFT to Determine Digital Straight Line Chain Codes, *Computer Graphics and Image Processing*, 18, pp. 359-368, 1982.
- LENSTRA LENSTRA LOVAVSZ — Factoring polynomial with rational coefficients, *Math. Annals* 261, 514-534, (1982).

- MACMAHON — Combinatorics
- 70 MANDELBROT B.B. — The Fractal Geometry of Nature, Ed. W.H. Freeman, N.Y. (1982).
- 71 MARKOFF A.— Sur une question de Jean Bernoulli, *Mathematische Annalen* Vol 19, 1882, pp 27-36.
- MENDES-FRANCE —
- 71 MORSE M. et HEDLUNG G.A. — Symbolics dynamics, *Amer. J. Math* 60 et 62, (1938) et (1940).
- MOSER W. et PACH J.— 100 research problems in discrete geometry, Mimeographed.
- 73 MULLER J.M. — Arithmétique des ordinateurs. Masson. Paris 1989.
- 74 NELSON E. — Internal set theory, *BAMS* 83, pp 1165-1198, (1977).
- NEUGENBAUMER —
- 75 NIJENHUIS A. et WILF H. — Representations of Integers by Linear Forms in Nonnegative Integers, *Journ. Number Theory* 4, pp. 98-106,(1972).
- 76 OSTER G. — The science of Moiré patterns. Edmund Scientific Co, Barrington N.J., U.S.A.
- 77 OVERMARS M. — Computational geometry on a grid an overview, *Nato ASI Series, Vol F40, Theoretical Foundations of Computer Graphics and CAO*, [Earnshaw Ed.], Springer-Verlag 1988.
- 78 PEITGEN H.O. et RICHTER P.H. — The Beauty of Fractals, Springer, (1986)
- 79 PAZ A. et SCHNORR C.P. — Approximating Integer Lattices by Lattices with Cyclic Factor Groups.
- PENROSE —
- 80 PHAM S. — Digital straight segments, *Comput. Vision Graph. Image Process.* 36, pp. 10-30, 1986.
- 81 PHAM S. — On the boundary of digital straight line segments, *Int. Comput. Graph. Conf. Tokyo (Avril 1986)*, pp. 79-109.
- 82 PHAM S.— Equations of digital straight lines, [T.L. KUNII Ed.] *Computer Graphics 1987*, pp 221-248.— Springer-Verlag 1987.[13]
- 83 PHAM S.— Parallel, overlapped, and intersected digital straight lines, *The Visual Computer*, 1988, vol 4, pp 247-258.
- 84 PICK G. — Geometrisches zur Zahlenlehre, *Sitzungsber, Lotos Prag.* (2) 19 (1870), 311-319.
- 85 PITTEWAY M.L.V. — Algorithm for drawing ellipses or hyperbolae with a digital plotter, *Comput. J.* 10 pp. 282-289, (1981).
- 86 POST M. et ZASSENHAUS H. — Algorithmic algebraic number theory, Cambridge University Press, Cambridge.

- PREPARATA F.P. et SHAMOS M.T. — Computational Geometry: an introduction, Springer, (1985).
- 87 RADEMACHER H.— Lectures on elementary number theory. Krieger. N.Y. 1977.
- 88 RADEMACHER H. et GROSSWALD E. — Dedekind Sums, The Carus Math. Monographs.
- 89 RANEY G.N. — On Continued Fractions and Finite Automata, Math. Ann. 206, pp. 265-283, 1973.
- 90 RAUZY G. — Suites à termes dans un alphabet fini, Sémin. Théorie Nombres, Bordeaux, pp 25-01, 25-16, (1982-83).
- 91 RAUZY G. — Mots infinis en arithmétique, Lecture Notes in Computer Science 192, pp. 165-171, (1985).
- 92 RAYLEIGH (Lord) — On the manufactures and theory of diffraction gratings. The London, Edinburgh and Dublin magazine and journal of science, Series 4, vol 47, n° 310, pp 81-93, (février 1874).
- 93 REEB G., REVEILLES J.P., TROESCH A. et URLACHER E. — Equations différentielles en nombres entiers, Rapport de Recherche IRMA Strasbourg, 1987.
- 94 REVEILLES J.P. — Les paliers des droites de Bresenham, Pixim 88, pp 81-101, Ed. Hermès, 1988.
- 95 ROBERT A. — Analyse non standard, Presses polytechniques romandes, (1985)
- 96 ROGERS D.F. — Procedural elements for computer graphics. McGraw Hill (1985).
- 97 ROSENFELD A. — Picture processing by computer, Ac. Press, N.Y. 1969.
- 98 ROSENFELD A. — Picture Languages, Ac. Press, New-York, 1979.
- 99 ROSENFELD A.— Arcs and curves in digital pictures, Journal of ACM, Vol 20, n°1, 1973, pp 81-87.
- 100 ROSENFELD A. — Digital straight line segments, IEEE Trans. Comput., C-23, 1974, pp 1264-1269.
- 101 ROSENFELD A. et MELTER R.A. — Digital Geometry, The Mathematical Intelligencer Vol. 11, N° 3 pp 69-72, Springer-Verlag N.Y. 1989.
- 102 ROSSER B. —A Generalization of the Euclidean Algorithm to Several Dimensions, Duke Math. J. 9, pp.59-95, 1942.
- 103 SEQUIN C.H. — Microfabrication on the Macintosh, USENIX Computer Graphics Workshop, Monterey, Nov. 1989.
- 104 SERIES C. —The Modular Surface and Continued Fractions, J. London Math. Soc. (2) 31, pp. 69-80, 1985.

- 105 SERIES C.— The Geometry of Markoff Numbers, *The Mathematical Intelligencer*, Vol 7, n° 3, 1985, pp 20-29.
- 106 SEROUL R. — Comment compiler ou interpréter une expression arithmétique, *L'ouvert* n° 59, juin 1990, pp 27-47.
- 107 SERRE J.P. — *Cours d'Arithmétique*, P.U.F., Paris, (1969).
- 108 SIEGEL K.L. — *Lectures on the Geometry of Numbers*. Springer. 1988.
- 109 SLATER N. — Gaps and steps for the sequence  $n\theta \pmod 1$ , *Proc. Camb. Phil. Soc.* n° 63, pp.1115- 1123, (1967).
- 110 SMITH H.J.S.— Note on continued fractions, *Messenger of Mathematics*, 2nd series, Vol 6, 1876, pp 1-14.
- 112 STANLEY R.P. — *Enumerative combinatorics — Vol. 1*, Wadsworth & Brooks/Cole, Monterey, California (1986).
- SZEKERES G.— Note on lattice points within a parallelepiped, *J. Lond. Math. Soc.* 12, pp36-39 (1936).
- 113 THEOCARIS P.S. — *Moiré fringes in strain analysis*, Pergamon Press (1969).
- 114 TROESCH A. — *Etude macroscopique de systèmes différentiels*. Proc. London Math. Soc. (1984).
- 115 TROESCH A. — Algorithmes de tracé de courbes utilisant des fonctions de contrôle, *Tagungsberichte Non Standard Analysis.- Bergische Universität, Gesamthochschule Wuppertal*, (1988).
- 116 VENKOV B. A. — *Elementary number theory*. Wolters-Noordhoff Pub., 1970.
- 117 VINOGRADOV J.M. — *Elements of number theory — Dover New York* (1954).
- 118 VUILLEMIN J. — Exact Real Computer Arithmetic with Continued Fractions, *IEEE Transactions on Computers* 39, N°8, pp. 1087-1105, Août 1990.
- 119 WILKINSON J.H.— *The algebraic eigenvalue problem*, Clarendon Press, Oxford, 1965.
- 120 WU L.D.— On the chain code of a line, *IEEE Trans. on Pattern Analysis and Machine intelligence*, Vol PAMI-4, n°3 May 82, pp 347-353.
- 121 WU X. et ROKNE J.G.— Double-Step Incremental Generation of Lines and Circles, *Computer Vision, Graphics and Image Processing*. 37, pp. 331-334, 1987.