Theoretical Computer Science 11 (1980) 207–220

ALGORITHME EXPLICITE POUR LA RECHERCHE DU P.G.C.D. DANS CERTAINS ANNEAUX PRINCIPAUX D'ENTIERS DE CORPS DE NOMBRES

B. BOUGAUT
Institut National des Sciences Appliquées, Rennes, France

Communiqué par M. Nivat

At first sight one may wonder why such a paper is published in TCS, since it looks pretty much like pure mathematics. The editor convinced himself however that this paper definitely brings new ideas about the Euclid's algorithm to compute the GCD and, as such, should interest all theoretically-minded computer scientists. More generally, the editor convinced himself that the relatively few mathematicians who try to use a computer to solve problems in algebra or number theory do contribute a lot to our knowledge of the 'computation phenomenon': he thus invites other papers of the same type as the present one to be submitted to TCS, as an attempt to fill in the unfortunate (and mainly sociological) gap between mathematics and theoretical computer science.

Reçu june 1978
Revisé june 1979

Abstract. We give a 'quasi-euclidean' division algorithm of some rings of integers in number fields; which we authorize to make use of the Euclid-algorithm for the computation of GCDs in these rings.

1. Introduction

L'algorithme d'Euclide—pour le calcul du P.G.C.D de deux entiers—est si ancien que le mot algorithme est utilisé, outre son sens habituel en informatique, pour désigner la fonction qui sert à contrôler la division dans les anneaux euclidiens. Rappelons qu'un anneau A est euclidien pour un algorithme ϕ (fonction à valeurs entières) si pour tout couple (a, b) d'éléments de A, $b \neq 0$, il existe q et r, éléments de A, tels que $a = bq + r$ et $\phi(r) < \phi(b)$. L'algorithme d'Euclide consiste à itérer ces divisions pour obtenir le P.G.C.D. (dernier reste non nul). Cet algorithme est couramment utilisé dans l'anneau des entiers (ϕ est alors la valeur absolue) et dans l'anneau des polynômes sur un corps (ϕ est alors le degré).

Bien que l'hypothèse de Riemann entraîne que tout anneau principal, d'entier algébrique, ayant une infinité d'unités, est euclidien, l'algorithme d'Euclide est rarement employé pour calculer le P.G.C.D. dans ces anneaux. En effet, il y a une obstruction à cette utilisation: même lorsque l'on connait la fonction algorithme ϕ, il faut savoir calculer le quotient et le reste de la division de deux éléments quelconques.

C'est pour éviter le recours à l'hypothèse de Riemann que nous avons introduit la notion d'anneau quasi-euclidien [2]. Dans un tel anneau, pour tout couple (a, b) d'éléments avec $b \neq 0$, on associe une division $(a = bq + r)$ et, comme pour l'algorithme classique d'Euclide, il existe une suite finie de telles divisions convergeant vers leur P.G.C.D.

Une théorème de Vaserštein [4] affirmant que, sauf quatre exceptions, tout anneau d'entiers de corps de nombres principal est quasi-euclidien, l'objet de cet article est d'indiquer une méthode explicite pour calculer le quotient et le reste de la division de deux éléments d'un tel anneau. Pour un anneau donné, les calculs préparatoires sont souvent longs (recouvrement d'un domaine fondamental ($F \subset \mathrm{Cf}(A)$; $F + A = \mathrm{Cf}(A)$) par des voisinages de 'rayon' $1/q$); et à ma connaissance ce travail n'a été effectué que pour quarantaine d'anneaux principaux d'entiers quadratiques. Mais une fois cette préparation effectuée, l'algorithme de la division, et donc l'algorithme (d'Euclide) du calcul du P.G.C.D. sont très rapides et pour ce dernier d'une vitesse comparable à celle de l'algorithme d'Euclide pour les entiers.

Après avoir rappelé au Paragraphe 2 les résultats connus sur les anneaux quasi-euclidiens, nous introduisons au Paragraphe 3 un algorithme de la division dans un anneau A à condition qu'il possède une partition euclidienne (Définition 5), propriété que nous montrons vérifiée au Paragraphe 4 pour les anneaux A_d, principaux d'entiers de corps quadratiques. Dans ce paragraphe nous donnons, à titre d'exemple, pour l'anneau A_{47} (en Exemple 2) la partition d'un domaine fondamental associée à son recouvrement par des voisinages. Le dernier paragraphe décrit la programmation de l'algorithme d'Euclide dans de tel anneau A_d.

2. Anneaux quasi-euclidiens

Tous les anneaux utilisés seront unitaires et communatifs.

Définition 1. Soit A un anneau, on appelle *quasi-algorithme* défini sur A une application $\phi: A^2 \to \mathbf{N}$ telle que pour tout $a \in A$ et tout $b \in A$, $b \neq 0$, il existe $q \in A$ et $r \in A$ avec $a = bq + r$ et $\phi(b, r) < \phi(a, b)$.

Définition 2. Un anneau A, non nécessairement intègre, est *quasi-euclidien* s'il existe un quasi-algorithme $\phi: A^2 \to \mathbf{N}$.

Définition 3. On dit que deux éléments a_1 et a_2, d'un anneau, possèdent une suite finie de *divisions généralisées convergeant vers leur P.G.C.D.* [2], s'il existe une suite finie $q_1, \ldots, q_n, a_3, \ldots, a_n$ d'éléments de A tels que $a_{i-1} = a_i q_i + a_{i+1}$ pour $2 \leq i < n$ et $a_{n-1} = q_n a_n + 0$. Remarquons que a_n est le P.G.C.D. de a_1 et de a_2, et que l'on peut écrire cette suite de divisions par le symbolisme suivant:

$$(a_1, a_3) \to (a_2, a_3) \to (a_3, a_4) \to \cdots \to (a_{n-1}, a_n) \to (a_n, 0).$$

Théorème 1. *Soit A un anneau non nécessairement intègre, les deux propositions suivantes sont équivalentes:*

(1) *il existe un quasi-algorithme $\phi: A^2 \to \mathbf{N}$, et par suite A est quasi-euclidien,*

(2) *pour tout $a \in A$ et tout $b \in A$, $b \neq 0$, il existe une suite finie de divisions généralisées convergeant vers leur P.G.C.D.*

Démonstration. (1) $\Rightarrow$ (2) à cause de la décroissance stricte des $\phi(a_i, a_{i+1})$.

(2) $\Rightarrow$ (1) nécessite la construction de l'application $\theta: A^2 \to \mathbf{N}$ définie par $\theta(a, b)$ égale le plus petit nombre de divisions ($a_{i-1} = a_i q_i + a_{i+1}$) apparaissant dans une suite finie de divisions généralisées convergeant vers P.G.C.D. (a, b). On démontre alors facilement que θ est un quasi-algorithme.

Exemples 1. Voici des exemples d'anneaux quasi-euclidens:

(a) Tout anneau euclidien est quasi-euclidien en prenant $\psi(a, b) = \phi(b)$.

(b) Tout anneau de valuation est quasi-euclidien en prenant $\psi: A^2 \to \{0, 1, 2\}$ définie par $\psi(a, 0) = 0$, $\psi(a, b) = 1$ si $b \neq 0$ et $v(a) \geq v(b)$, et $\psi(a, b) = 2$ dans les autres cas.

(c) Tout anneau principal, de type arithmétique, ayant une infinité d'unités est quasi-euclidien. La démonstration de cet exemple est basée sur un résultat de Vaserštein [4] et un théorème sur le groupe $GE_n(A)$ ([2, Théorème 17]). D'autre part, il faut utiliser l'hypothèse de Riemann pour démontrer que ces anneaux sont euclidiens. Dans ce cadre il faut signaler que l'on ignore actuellement s'il existe des anneaux principaux quasi-euclidiens et non euclidiens.

Proposition 1. *Dans un anneau quasi-euclidien, deux éléments quelconques ont un P.G.C.D.*

C'est une conséquence du Théorème 1.

Remarque 1. Comme on se restreint ici aux anneaux principaux des entiers de corps de nombres, l'intégrité de ces anneaux donne l'unicité du P.G.C.D. aux unités près.

Proposition 2. *Tout anneau, non nécessairement intègre, quasi-euclidien est un anneau de Bezout.*

Rappel. Un anneau de Bezout est un anneau dans lequel tout idéal de type fini est principal

La démonstration de cette proposition se trouve dans [2].

Le théorème précédent nous a montré que les anneaux quasi-euclidiens sont essentiellement les anneaux dans lesquels il existe un algorithme 'd'Euclide' pour le calcul du P.G.C.D., cet algorithme étant basé sur la division quasi-euclidienne. Nous allons montrer comment on peut construire cette division pour les anneaux principaux d'entiers de corps de nombres qui sont quasi-euclidiens d'après (c) des Exemple 1.

3. Principe de l'algorithme de la division dans un anneau A principal d'entiers de corps de nombres

Définition 4. Dans le corps $\mathrm{Cf}(A)$ des fractions de A, appelons *domaine fondamental* F, une partie de $\mathrm{Cf}(A)$ admettant l'origine comme centre de symétrie, qui par translation ($x \to x+q$, $q \in A$) recouvre $\mathrm{Cf}(A)$ et dont l'intersection avec l'un quelconque de ses translatés est vide. Par exemple, dans l'anneau A_d des entiers de $\mathbf{Q}(\sqrt{d})$, pour $d \equiv 2$ ou $3 \pmod 4$ on peut prendre $F = \{a+b\sqrt{d}, (a,b) \in (\mathbf{Q} \cap]-\frac{1}{2}, \frac{1}{2}])^2\}$.

Définition 5. Une *partition euclidienne* d'un anneau A consiste en un nombre fini de couples $(T_i, s_i)_{i=1,\ldots,n}$ et de triplets $(T'_j, t_j, u_j)_{j=1,\ldots,p}$ tels que les éléments s_i, t_j, u_j appartiennent à A avec $u_j \neq 0$ pour $j = 1, \ldots, p$ et tels que les sous-ensembles T_i et T'_j forment une partition d'un domaine fondamental F de A.

Définition 6. Dans tout anneau A, possédant une partition euclidienne, pour tout couple (a, b) d'éléments non nuls de A on définit une *division généralisée de a par b* par le procédé suivant:

Appelons $\lambda_{a/b}$ l'unique translation de A telle que $a/b - \lambda_{a/b} \in F$; s'il existe un j tel que $b/a + t_j \in T'_j$, on pose $q = u_j$ et $r = a - bq$; sinon, ou bien, il existe un i tel que $a/b - \lambda_{a/b} \in T_i$ et on pose $q = s_i + \lambda_{a/b}$ et $r = a - bq$; ou bien il existe un j tel que $a/b - \lambda_{a/b} \in T'_j$ et on pose $q = t_j + \lambda_{a/b}$ et $r = a - bq$.

3.1. Algorithme de la division

Définition 7. On appelle *norme* définie sur un anneau intègre A, une application multiplicative $\mu^0 : A \to \mathbf{N}$ telle que $\mu^0(x) = 0$ si et seulement si $x = 0$. Cette application s'étend naturellement en une application $\mu : \mathrm{Cf}(A) \to \mathbf{Q}^+$.

Introduisons les *voisinages V et W*. Pour $s \in A$, posons $V(s) = \{x \in \mathrm{Cf}(A);\ \mu(x-s) < 1\}$ et pour t et $u \neq 0$ éléments de A, posons $W(t,u) = \{x \in \mathrm{Cf}(A);\ \mu(x-(t+1/u)) < 1/\mu(u)\}$.

Théorème 2. *Soit A un anneau intègre, possédant une norme μ et une partition euclidienne. Si pour tout $i \in \{1, \ldots, n\}$, on a $T_i \subset V(s_i)$ et pour tout $j \in \{1, \ldots, p\}$ on a $T'_j \subset W(t_j, u_j)$ et $T'_j \cap V(t_j) = \emptyset$; Alors*

(1) *pour tout $a \in A$ et tout $b \in A$, $b \neq 0$, la suite de divisions associées à la partition euclidienne converge, en un nombre fini de pas, vers le P.G.C.D. de a et de b,*

(2) *il existe une application $\phi : A^2 \to \mathbf{N}$ telle que ces divisions associées à la partition euclidienne soient des divisions pour le quasi-algorithme ϕ.*

Démonstration. Comme (2) implique (1) à cause de la décroissance stricte des $\phi(a_i, a_{i+1})$, il suffit de démontrer (2). Auparavant donnons la valeur de $\phi(x, y)$ et démontrons un lemme.

Pour tout $(x, y) \in A^2$ posons $\phi(x, y) = 2\mu(y)$ sauf pour les couples (x, y) tels qu'il existe $j \in \{1, \ldots, p\}$ avec $y/x + t_j \in T'_j \subset W(t_j, u_j)$ et dans ce cas $\phi(x, y) = 2\mu(x) - 1$.

Lemme 1. *Si* $\phi(x, y) = 2\mu(x) - 1$, *on a nécessairement* $\mu(y) \geq \mu(x)$.

Démonstration du lemme. La définition de l'application ϕ nous indique qu'il existe $j \in \{1, \ldots, p\}$ tel que $y/x + t_j \in T'_j \subset W(t_j, u_j)$.

Comme par définition des ensembles T'_j, $T'_j \cap V(t_j) = \emptyset$, on a $y/x + t_k \notin V(t_j)$; c'est à dire $\mu(y/x + t_j - t_j) \geq 1$. D'où le résultat.

Pour démontrer l'assertion (2) du théorème, considérons un couple quelconque (a, b) d'éléments de $A \times A^*$ et montrons que le quotient et le reste de la division associée à la partition euclidienne vérifie $a = bq + r$ avec $\phi(b, r) < \phi(a, b)$.

Pour plus de clarté, nous établirons ce résultat en raisonnant sur la parité de $\phi(a, b)$:

(1) $\phi(a, b) = 2\mu(b)$. Il existe une translation unique $\lambda_{a/b} \in A$ telle que $a/b - \lambda_{a/b} \in F$. D'où deux cas:

- il existe $i \in \{1, \ldots, n\}$ tel que $a/b - \lambda_{a/b} \in T_i \subset V(s_i)$. On a donc $\mu(a/b - \lambda_{a/b} - s_i) < 1$. En posant $q = \lambda_{a/b} + s_i$ et $r = a - bq$, on obtient $a = bq + r$ avec $\mu(r) < \mu(b)$. D'autre part, $r/b = (a - bq)/b = a/b - q$ donc $r/b + s_i = a/b - \lambda_{a/b} \in T_i$ et par suite $\phi(b, r) = 2\mu(r)$. Dans ce cas, on a bien $a = bq + r$ avec $\phi(b, r) < \phi(a, b)$;
- Il existe $j \in \{1, \ldots, p\}$ tel que $a/b - \lambda_{a/b} \in T'_j \subset W(t_j, u_j)$. Puisque $a/b - \lambda_{a/b} \in W(t_j, u_j)$, en posant $q = \lambda_{a/b} + t_j$ et $r = a - bq$, on a $a = bq + r$. D'autre part $r/b = a/b - q$ d'où $r/b + t_j = a/b - \lambda_{a/b} \in T'_j$. Donc, d'après la définition de ϕ, on a $\phi(b, r) = 2\mu(b) - 1$. Dans ce cas, on a encore $a = bq + r$ avec $\phi(b, r) < \phi(a, b)$.

(2) $\phi(a, b) = 2\mu(a) - 1$. Puisque $b/a + t_j \in T'_j \subset W(t_j, u_j)$, en posant $q = u_j$ et $r = a - bq$, on a $a = bq + r$. Il reste alors à calculer $\phi(b, r)$ puis à le comparer à $\phi(a, b)$. Comme

$$\mu\left(\frac{b}{a} - \frac{1}{u_j}\right) = \mu\left(\frac{b}{a} + t_j - \left(t_j + \frac{1}{u_j}\right)\right) < \frac{1}{\mu(u_j)},$$

on a $\mu(r) = \mu(-r) = \mu(bu_j - a) < \mu(a)$. Donc $\mu(r) \leq \mu(a) - 1$ ou encore $2\mu(r) \leq 2\mu(a) - 2 < 2\mu(a) - 1$.

D'autre part, le Lemme 1 entraîne $\mu(b) \geq \mu(a)$. Si $\phi(b, r) = 2\mu(b) - 1$, on aurait de même $\mu(r) \geq \mu(b) \geq \mu(a)$, ce qui est contraire à nos conclusions précédentes. Nous en déduisons que $\phi(b, r) = 2\mu(r)$. Dans ce cas, nous avons encore $a = bq + r$ avec $\phi(b, r) = 2\mu(r) < 2\mu(a) - 1 = \phi(a, b)$.

ϕ est bien un quasi-algorithme ce qui termine la démonstration du théorème et montre que A est quasi-euclidien.

Notons que le quasi-algorithme ϕ utilisé n'est pas minimal. D'autre part, dans le cas des anneaux d'entiers de corps de nombres que nous considérerons plus tard, on

pourra prendre pour μ la valeur absolue de la norme, F est isomorphe à $\mathbf{Q}^n/\mathbf{Z}^n$ et les régions T_i et T'_j sont alors définies par un système simple d'inégalités. Dans ces cas la division est donc facile à effectuer.

Corollaire 1. *Les anneaux vérifiant les hypothèses du Théorème 2 sont de Bezout.*

Ce résultat est immédiat, compte tenu du Proposition 2.

Remarque importante. La démonstration du Théorème 2 permet de donner un algorithme pour le calcul du P.G.C.D.

Pour appliquer un algorithme pour la recherche du P.G.C.D. l'important dans la division quasi-euclidienne est de disposer du quotient et du reste plutôt que de connaître la valeur prise par les $\phi(a_i, a_{i+1})$. La donnée d'une partition euclidienne satisfaisant aux conditions du Théorème 2 donne explicitement, pour tout a et tout b, $b \neq 0$, le quotient et le reste de la division quasi-euclidienne de a par b. Au contraire, dans les anneaux d'entiers algébriques, même euclidiens pour la norme, la connaissance et le calcul facile de cette norme ne donnent aucune méthode rapide pour exhiber le quotient et le reste de la division de a par b (il faut en effet chercher, par exploration systématique, dans la classe de a modulo bA, un élément r tel que $|N(r)| < |N(b)|$, puis calculer la valeur correspondante de $q \in A$ vérifiant $a = bq + r$). Ainsi, l'algorithme donné par le Théorème 2 est intéressant même dans le cas des anneaux euclidiens pour la norme.

Cependant pour utiliser le Théorème 2, il faut connaître une partition euclidienne convenable: c'est l'objet du paragraphe suivant.

4. Construction d'une partition euclidienne dans un anneau A principal d'entiers de corps de nombres

Nous allons montrer de quelle manière il est possible de construire une partition euclidienne.

A étant un anneau d'entiers de corps de nombres, A est une $\mathbf{Z}$-algèbre, libre de dimension finie n possédant donc une norme $N(\cdot)$.

On peut prolonger cette norme en une application μ définie sur $\mathbf{R}^n$ en l'étendant d'abord à $\mathbf{Q}^n$ puis par continuité à $\mathbf{R}^n$.

Puisque le choix d'une base de A définit un isomorphisme entre A et $\mathbf{Z}^n$, on a $\mathbf{C}(A) \simeq \mathbf{Q}^n \subset \mathbf{R}^n$ et le domaine fondamental F est alors isomorphe à une intersection de $\mathbf{R}^n$ avec un cube de dimension n.

Les techniques classiques de Géométrie des Nombres permettent, alors, de trouver les voisinages $V(s_i)$ et $W(t_j, u_j)$ recouvrant F.

Proposition 3. *Le recouvrement du domaine fondamental F par des voisinages $V(s_i)$*

et $W(t_j, u_j)$ permet de construire une partition euclidienne vérifiant les conditions du Théorème 2.

On affine le recouvrement en prenant des sous-ensembles R_k des voisinages, formant une partition de F. A ce stade l'anneau A possède, de manière évidente, une partition euclidienne.

Pour que cette partition euclidienne vérifie les conditions du Théorème 2, il suffit de poser $T_i = R_i \cap V(s_i)$ ou $T_j = R_j \cap V(t_j)$ et $T'_j = R_j - V(t_j)$. Pour faciliter la programmation, nous conservons la distinction entre les régions T et T' mais nous supprimons les régions qui sont vides et nous changeons la numérotation pour la rendre conhérente.

Remarque 2. Un choix judicieux des régions R_i permet de limiter les erreurs de calculs. En effet, il suffit de choisir les frontières des régions R_i de façon à laisser de part et d'autre de la frontière entre R_i et R_{i+1} une bande, d'épaisseur e, appartenant aux deux voisinages (voir Fig. 1).

De même si la frontière de deux voisinages est issue d'un même point (par exemple dans notre futur exemple A_{47} pour le point $\frac{1}{2}+\frac{1}{2}\sqrt{\frac{5}{47}}$ il est préférable pour la même raison, de rechercher un nouveau voisinage afin de définir une nouvelle région centrée sur ce point. Ces exemples montrent que l'on peut associer beaucoup de partitions euclidiennes à un anneau. C'est la précision des calculs que l'on veut obtenir (par rapport à l'ordinateur utilisé) qui nous guidera dans le choix de l'épaisseur e et par suite dans le choix du recouvrement.

Proposition 4. *Nous allons étudier valeurs de d telles que les anneaux A_d principaux (des entiers du corps $\mathbf{Q}(\sqrt{d})$) possèdent une partition euclidienne satisfaisant aux conditions du Théorème 2.*

Le domaine fondamental F de ces anneaux admettant deux axes de symétrie, il suffit que ces anneaux possèdent un recouvrement d'une partie E de F qui donnera F par les symétries précitées:

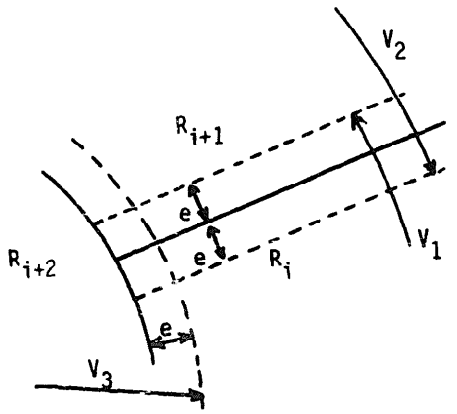

Fig. 1.

(1) *Pour les valeurs de d qui rendent A_d euclidien*

$$d = -1, -2, -3, -7, -11;$$

$$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Pour montrer que ces anneaux sont euclidiens, on utilise un recouvrement du domaine fondamental par des voisinages $V(s_i)$. Barnes et Swinnerton-Dyer en donnent, dans [1], une bibliographie presque exhaustive.

Remarquons que les régions du domaine fondamental, qui ne sont pas facilement recouvertes par des voisinages $V(s_i)$, le sont par contre par des voisinages $W(t_j, u_j)$.

(2) *Pour $d = 14, 22, 43, 46, 53, 61, 69$.* Cooke, dans [3], a donné un recouvrement du domaine fondamental et a esquissé ce recouvrement pour $d = 23, 31, 38, 77, 89, 93, 97, 113, 129, 133, 137, 181, 253$.

Remarquons que, ces anneaux vérifiant les conditions du Théorème 2, sont quasi-euclidiens.

(3) Nous allons montrer maintenant que l'on peut trouver une partition euclidienne vérifiant les conditions du Théorème 2 pour la première valeur non donnée par Cooke *soit $d = 47$.*

Exemple 2. Nous avons montré dans [2] que le recouvrement du domaine fondamental $F = \{\xi + \eta\sqrt{47},\ (\xi, \eta) \in (\mathbf{Q} \cap [-\frac{1}{2}, \frac{1}{2}])^2\}$ de A_{47} s'obtient par les voisinages:

$$V(s_i) \quad \text{pour } s_i \in \{0, \pm 1, \pm 2, \pm 16 \pm 2\sqrt{47}, \pm 220 \pm 32\sqrt{47}\}$$

$$W(t_j, u_j) \quad \text{pour } (t_j, u_j) \in \{(\pm 2, \pm 14 \pm 2\sqrt{47}), (\pm 16 \pm 2\sqrt{47}, \pm 144 \pm 21\sqrt{47}), (\pm 3, \pm 7 \pm \sqrt{47}), (\pm 5, \pm 7 \pm \sqrt{47}), (\pm 1, \pm 14 \pm 2\sqrt{47}), (\pm 12 \pm 2\sqrt{47}, \pm 192 \pm 28\sqrt{47}), (\pm 358 \pm 52\sqrt{47}, \pm 3942 \pm 575\sqrt{47})\}.$$

Puis nous définissons les régions R_i par (voir Fig. 2)

$$R_0 = \{(0, 0)\},$$

$$R_1 = \{(x, y) \in E - R_0,\ y \leqslant \tfrac{1}{2}\sqrt{\tfrac{5}{47}}\},$$

$$R_2 = \{(x, y) \in E,\ \tfrac{1}{2}\sqrt{\tfrac{5}{47}} < y \leqslant 0.2\},$$

$$R_3 = \{x, y) \in E,\ 0.2 < y \leqslant 0.3\},$$

$$R_4 = \left\{(x, y) \in E,\ y - \frac{x}{\sqrt{47}} + \frac{1}{2\sqrt{47}} - 0.392 < 0,\right.$$

$$\left. y - \frac{x}{\sqrt{47}} - \frac{1.8}{\sqrt{47}} > 0 \text{ et } y > 0.3\right\},$$

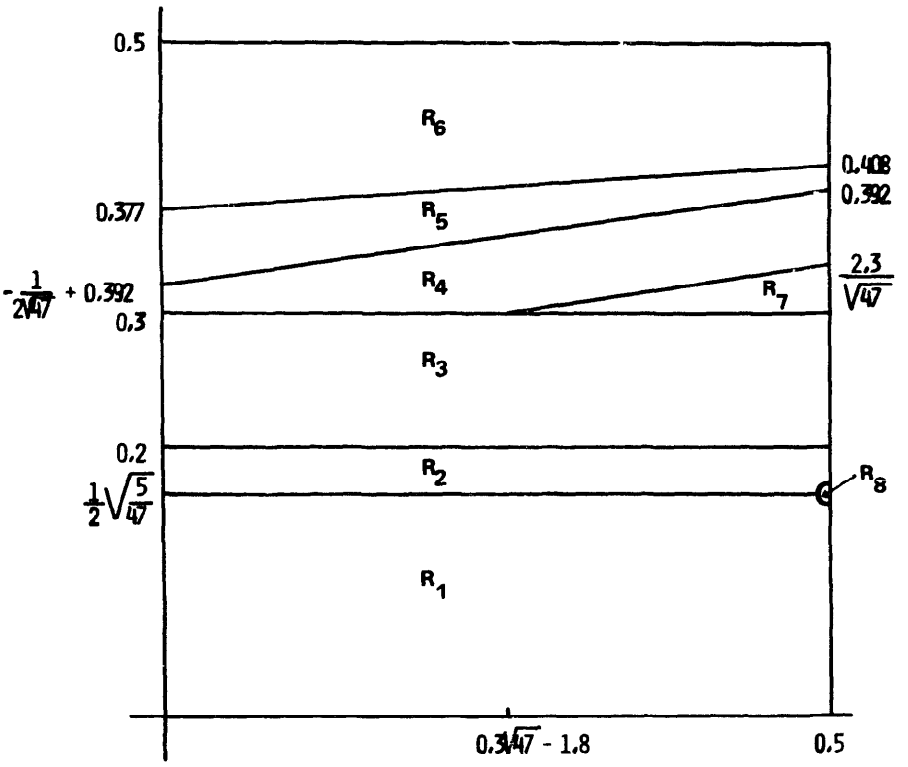

Fig. 2.

$$R_5 = \left\{(x, y) \in E,\ y - \frac{x}{\sqrt{47}} + \frac{1}{2\sqrt{47}} - 0.392 \geqslant 0 \text{ et } y - \frac{62}{1000}x - \frac{377}{1000} < 0\right\},$$

$$R_6 = \{(x, y) \in E,\ y - \tfrac{62}{1000}x - \tfrac{377}{1000} \geqslant 0 \text{ et } y \leqslant \tfrac{1}{2}\},$$

$$R_7 = \left\{(x, y) \in E,\ y - \frac{x}{\sqrt{47}} - \frac{1.8}{2\sqrt{47}} \leqslant 0 \text{ et } y > 0.3\right\},$$

$$R_8 = \{(x, y) \in E,\ (x - 0.5)^2 + (y - \tfrac{1}{2}\sqrt{\tfrac{5}{47}})^2 \leqslant 10^{-4}\}.$$

La région R_7 se subdivise en quatre sous-ensembles (voir Fig. 3):

$$R_7^{\mathrm{I}} = \left\{(x, y) \in R_7,\ y - \frac{x}{\sqrt{47}} - \frac{1.8}{\sqrt{47}} \leqslant 0 \text{ et } y - \frac{x}{\sqrt{47}} - 0.254 \geqslant 0\right\},$$

$$R_7^{\mathrm{II}} = \left\{(x, y) \in R_7,\ y - \frac{x}{\sqrt{47}} - 0.254 < 0 \text{ et } y + \frac{x}{\sqrt{47}} - 0.3828 \leqslant 0\right\},$$

$$R_7^{\mathrm{III}} = \left\{(x, y) \in R_7,\ y - \frac{x}{\sqrt{47}} - 0.254 < 0,\right.$$

$$\left. y + \frac{x}{\sqrt{47}} - 0.3828 > 0 \text{ et } y \geqslant 0.317\right\},$$

$$R_7^{\mathrm{IV}} = \left\{(x, y) \in R_7,\ y < 0.317 \text{ et } y + \frac{x}{\sqrt{47}} - 0.3828 > 0\right\}.$$

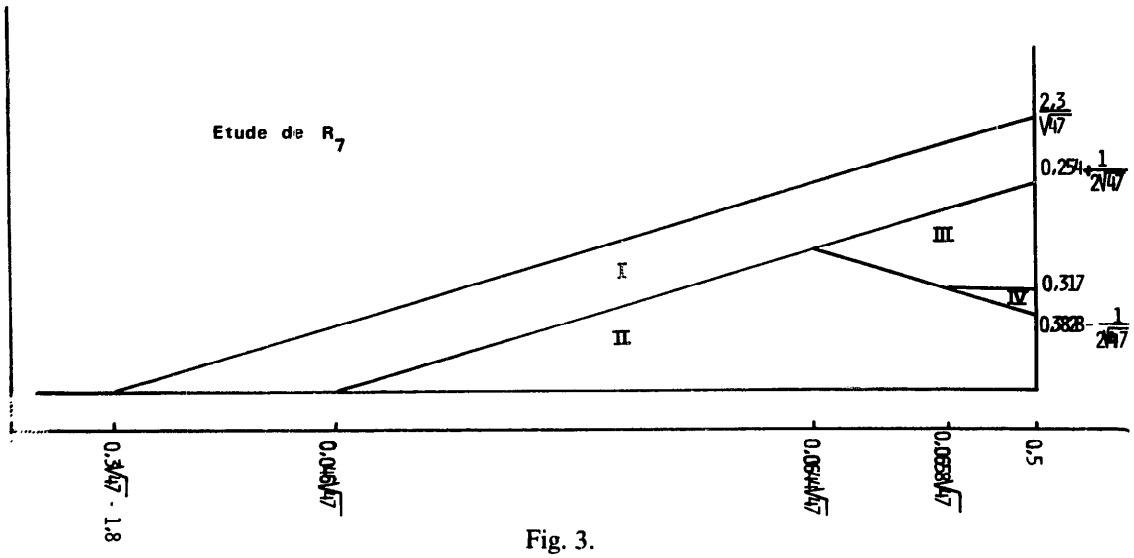

Fig. 3.

La partition euclidienne de F satisfaisant aux conditions du Théorème 2 est obtenue par les régions $\pm T_i$, $\pm T'_j$, $\pm\sigma(T_i)$, $\pm\sigma(T'_j)$, ainsi définies:

$$T_1 = \{0\} \subset V\{0\}, \qquad T_2 = R_1 \subset V(1), \qquad T_3 = R_2 \subset V(-1),$$

$$T_4 = V(2) \cap R_3 \subset V(2), \qquad T_5 = R_4 \subset V(-2),$$

$$T_6 = R_5 \cap V(-16-2\sqrt{47}) \subset V(-16-2\sqrt{47}),$$

$$T_7 = R_8 \subset V(-220, -32),$$

$$T'_1 = [R_3 - (V(2) \cap R_3)] \subset W(2, -14-2\sqrt{47}),$$

$$T'_2 = [R_5 - (V(16-2\sqrt{47}) \cap R_5)] \subset W(-16-2\sqrt{47}, 144-21\sqrt{47}),$$

$$T'_3 = R_6 \subset W(-3, 7-\sqrt{47}), \qquad T'_4 = R_7^{\mathrm{I}} \subset W(5, -7-\sqrt{47}),$$

$$T'_5 = R_7^{\mathrm{II}} \subset W(-1, 14-2\sqrt{47}),$$

$$T'_6 = R_7^{\mathrm{III}} \subset W(-12+2\sqrt{47}, 192+28\sqrt{47}),$$

$$T'_7 = R_7^{\mathrm{IV}} \subset \mathrm{W}(-358-52\sqrt{47}, -3942+575\sqrt{47}).$$

Enfin appelons σ l'automorphisme de $\mathbf{Q}(\sqrt{47})$ qui transforme $a+b\sqrt{47}$ en $a-b\sqrt{47}$.

Le choix présenté ici donne une zone d'épaisseur $e > 0.01$ de recouvrement (Remarque 2) des régions T par les voisinages.

Rappelons que pour effectuer la division de a par $b \neq 0$, il suffit de chercher à quelle région ($\pm T_i$ ou $\pm T'_i$ ou $\pm\sigma(T_i)$ ou $\pm\sigma(T'_i)$) appartient le représentant module 1 de a/b ou de b/a. On obtient alors immédiatement le quotient et le reste de la division 'quasi-euclidienne'.

L'anneau $\mathbf{Z}(\sqrt{47})$, vérifiant les hypothèses du Théorème 2, est quasi-euclidien.

(4) Pour les autres valeurs positives de d telles que A_d soit principal et pour les autres anneaux principaux de corps de nombres ayant une infinité d'unités, un

théorème de Vaserštein [4] a permis de montrer dans [2] que ces anneaux sont quasi-euclidiens. On peut donc espérer trouver facilement un recouvrement d'un domaine fondamental de ces anneaux et savoir effectuer des divisions dans ces anneaux.

5. Algorithme du P.G.C.D. dans les anneaux principaux A_d

Réalisé pour un anneau principal de la forme A_d (entier d'une extension quadratique de **Q**), ce programme est la traduction classique de l'algorithme d'Euclide pour le calcul du P.G.C.D. en utilisant les quotients et les restes donnés par le Théorème 2.

5.1. Algorithme

Dans la présentation de ce programme nous noterons entre parenthèses et en italique son application à $d = 47$:

(1) *Répresentation des éléments*

- Entier de A_d '$a_1 + a_2 e$': le couple d'entier $(a_1, a_2) = a$;
- Entier de Cf(A_d): le couple de réels ou de rationnels $(x_1, x_2) = x$.

(2) *Données d'entrée*

- Donner d et une base $(1, e)$ sur **Z** de A_d *($d = 47$, $e = \sqrt{47}$)*;
- Donner l'unité fondamentale $\varepsilon = \varepsilon_1 + \varepsilon_2 e$ *($\varepsilon_1 = 48$, $\varepsilon_2 = 7$)*;
- Définition des voisinages $V(s_i)$ et $W(t_j, u_j)$ *(voir Exemple 2)*;
- Définition des régions T_i et T'_i *(sur E uniquement; voir l'ensemble des inegalités de l'Exemple 2)*.

(3) *Sous-programmes de base*

- Opération addition: addition de deux couples dans A_d et dans Cf(A_d);
- Opération multiplication: donner la table de multiplication dans A_d et dans Cf(A_d) *($e^2 = 47$)*;
- Norme d'un élément $z = a + be$: $N(z) = z\bar{z}$ *($a^2 - 47b^2$)*;
- Opération inverse de $z = a + be$: $\bar{z}/N(z)$.

(4) *Programme principal.* x, y, et z représentent des réels, et les autres lettres des entiers.

(A_1) lire $a = (a_1, a_2)$; $b = (b_1, b_2)$;

(A_2) si $b = (0, 0)$ alors faire (P.G.C.D. $\leftarrow a$; STOP;) FIN;

(A_3) $a \leftarrow$ SIMPL(a); $b \leftarrow$ SIMPL(b); — la fonction SIMPL est destinée à réduire la taille des éléments et sera étudiée ci-dessous;

(A_4) $x \leftarrow b/a$;

(A_5) pur $j = 1$ à J_2 faire
si $x + t(j) \in T'_j$ alors faire PHI$(a, b) \leftarrow 2|N(a)| - 1$; $q \leftarrow u_j$;
$r \leftarrow a - bq$; $a \leftarrow b$; $b \leftarrow r$; aller en A_2; FIN; FIN;

(A_6) $y \leftarrow a/b$; $k \leftarrow [y]$; $z \leftarrow a/b - k$; PHI$(a, b) \leftarrow 2|N(b)|$;
pour $i = 1$ à I_1 faire
si $z \in T_i$ alors faire $q \leftarrow k + s(i)$; $r \leftarrow a - bq$; $a \leftarrow b$; $b \leftarrow r$; aller en A_2; FIN;

Pour $j = 1$ à J_2 faire
si $z \in T'_j$ alors faire $q \leftarrow k + t(j)$; $r \leftarrow a - bq$; $a \leftarrow b$; $b \leftarrow r$; aller en A_2; FIN;
FIN;

(5) *Programme auxiliaire*

- SIMPL(a)

(S_1) Rappelons que $a = (a_1, a_2)$;

si $\dfrac{\varepsilon_2 d}{\varepsilon_1 + 1} < \left|\dfrac{a_1}{a_2}\right| < \dfrac{\varepsilon_1 + 1}{\varepsilon_2}$ alors faire
si $a_1 a_2 > 0$ alors faire $a \leftarrow a\bar{\varepsilon}$; aller en S_1; FIN; FIN;
sinon faire $a \leftarrow a\varepsilon$; aller en S_1; FIN; FIN;
sinon SIMPL(a) $\leftarrow a$; FIN;

Ce programme SIMPL, en divisant éventuellement un élément de A_d par une unité, permet que la taille des restes successifs ne dépasse pas sensiblement la taille des données initiales. Il permet ainsi d'éviter les dépassements de capacité et rend inutile l'emploi de la multiple précision de grande longueur pour les calculs.

Remarque 3. Afin de diminuer le temps de calcul, on a intérêt à ne considérer que le sous-ensemble E (cf. Proposition 4) du domaine fondamental F; ce qui alourdit l'écriture du programme par l'introduction de nombreux calculs de valeurs absolues et de signes auxiliaires. Par contre, il est souhaitable de modifier le programme pour calculer la valeur de PHI(b, r)—voir le Théorème 2 pour sa définition—et de la comparer à sa valeur théorique qui est égale à celle de PHI(a, b) du passage suivant. En pratique les erreurs d'arrondi peuvent donner des résultats différents et nous allons voir que cela ne change pas le bon déroulement du calcul du P.G.C.D.

5.2. Stabilité du calcul du P.G.C.D. relative aux erreurs de calculs

La précision des calculs étant limitée, il se peut qu'une erreur se produise dans le positionnement du quotient $y = a/b$ (mod 1). Si y devant appartenir à C_1, est placé, par suite d'erreurs de calculs dans une région voisine C_2 de C_1 (on a $y + \xi \in C_2$), la division s'effectuera avec le quotient et le reste associés à C_2. Ce n'est pas gênant si le recouvrement de C_2 par son voisinage $V(s_2)$ ou $W(t_2, u_2)$ laisse une bande frontalière d'épaisseur $e \geqslant \xi$ recouvrant C_1 (voir Fig. 4).

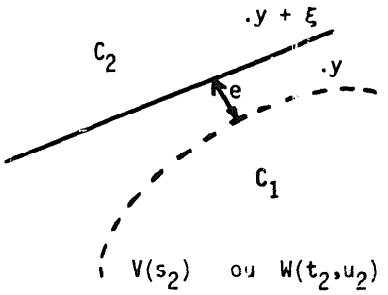

Fig. 4.

Dans la majorité des cas ce dépassement existe et l'utilisation de la multiple précision permet de réduire l'épaisseur. Ainsi sur un IRIS 80, on obtient $e \leqslant 10^{-6}$ en employant la double précision.

Si l'erreur de positionnement se produit en vérifiant que $b/a + t(j) \in T'_j$—soit pour le calcul de PHI(a, b)—on démontre facilement que la même condition est suffisante. Mais si l'erreur se produit lors du calcul du PHI(b, r), elle peut être en opposition avec le résultat obtenu pour le calcul de PHI(a, b); (par exemple, $a/b \pmod 1 \in T'_1$, donc PHI$(a, b) = 2|N(b)|$ et on devrait obtenir PHI$(b, r) = 2|N(a)| - 1$ alors que le calcul de PHI(b, r) peut donner $2|N(r)|$ et être supérieur à $2|N(b)|$). De plus l'incidence de cette erreur ne peut apparaître que lors de la division suivante. C'est pour ces raisons que nous considérons seulement une décroissance globale de l'ensemble des valeurs de l'application PHI au lieu d'une stricte décroissance des PHI(r_n, r_{n+1}). Cette modification peut augmenter légèrement le nombre des itérations de l'algorithme: ce qui n'est pas gênant pour le calcul du P.G.C.D.

5.3. Résultats concrets

Voici, pour terminer, des résultats concrets:

(a) Pour donner un exemple du temps de calcul (avec l'IRIS 80 de l'Université de Rennes I), une recherche de quatre P.G.C.D. dans A_{47}, comportant 54 divisions à effectuer, a demandé moins de $\frac{4}{100}$ de minute.

(b) Enfin voici deux exemples de calcul de P.G.C.D. dans A_{47}:

Exemple 3. Calcul du P.G.C.D. de $A = (17, 101)$ et de $B = (31, 71)$.

$(17, 101) = (31, 71) \times (2, 0) + (-45, -41)$
avec PHI$(B, R) = 153964$ et PHI$(A, B) = 471932$

$(31, 71) = (-45, -41) \times (-1, 0) + (-14, 30)$
avec PHI$(B, R) = 84208$ et PHI$(A, B) = 153964$

$(-45, -41) = (-14, 30) \times (-2, 0) + (-73, 19)$
avec PHI$(B, R) = 23276$ et PHI$(A, B) = 84208$

$(-14, 30) = (-73, 19) \times (1, 0) + (59, 11)$
avec PHI$(B, R) = 4412$ et PHI$(A, B) = 23276$

$(-73, 19) = (59, 11) \times (7, -1) + (31, 1)$
avec PHI$(B, R) = 1828$ et PHI$(A, B) = 4412$

$(59, 11) = (31, 1) \times (0, 0) + (59, 11)$ avec PHI$(B, R) = 1827$ et PHI$(A, B) = 1828$

$(31, 1) = (59, 11) \times (14, -2) + (239, -35)$
avec PHI$(B, R) = 908$ et PHI$(A, B) = 1827$

$(239, -35) = (-43, -7) \times (48, -7)$

$(59, 11) = (-43, -7) \times (-3, 0) + (-70, -10)$
avec PHI$(B, R) = 400$ et PHI$(A, B) = 908$

$(-43, -7) = (-70, -10) \times (-3, 0) + (-253, -37)$
avec PHI$(B, R) = 399$ et PHI$(A, B) = 400$

$(-253, -37) = (29, -5) \times (48, 7)$
$(-70, -10) = (29, -5) \times (14, 2) + (-6, 2)$
avec PHI$(B, R) = 304$ et PHI$(A, B) = 668$
$(29, -5) = (-6, 2) \times (-3, 0) + (11, 1)$ avec PHI$(B, R) = 148$ et PHI$(A, B) = 304$
$(-6, 2) = (11, 1) \times (14, -2) + (-66, 10)$
avec PHI$(B, R) = 147$ et PHI$(A, B) = 148$
$(11, 1) = (-66, 10) \times (-144, -21) + (377, 55)$
avec PHI$(B, R) = 92$ et PHI$(A, B) = 147$

$(377, 55) = (1, 1) \times (48, 7)$
$(-66, 10) = (1, 1) \times (14, -2) + (14, -2)$ avec PHI$(B, R) = 16$ et PHI$(A, B) = 92$
$(1, 1) = (14, -2) \times (14, 2) + (-7, 1)$ avec PHI$(B, R) = 4$ et PHI$(A, B) = 16$
$(14, -2) = (-7, 1) \times (-2, 0) + (0, 0)$ avec PHI$(B, R) = 0$ et PHI$(A, B) = 4$

Le P.G.C.D. de A et de B est: $(-7, 1)$

Exemple 4. Calcul du P.G.C.D. de $A = (2024228, -295264)$ et de $B = (49018424, -7150072)$.

$(2024228, -295264) = (32, 4) \times (48, -7)^3$
$(49018424, -7150072) = (56, -8) \times (48, -7)^3$
$(32, 4) = (56, -8) \times (24, 4) + (192, -28)$
avec PHI$(B, R) = 32$ et PHI$(A, B) = 256$

$(192, -28) = (4, 0) \times (48, -7)$
$(56, -8) = (4, 0) \times (14, -2) + (0, 0)$ avec PHI$(B, R) = 0$ et PHI$(A, B) = 32$

Le P.G.C.D. de A et de B est: $(4, 0)$.

Bibliographie

[1] E.S. Barnes et H.P.F. Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms (I), *Acta Math.* **87** (1, 2) (1952).
[2] B. Bougaut, Anneaux quasi-euclidiens, Thèse, Université de Poitiers (1976).
[3] G. Cooke, A weakening of the euclidean property for integral domains and applications to algebraic number theory, *J. Reine Angew. Math.* **282** (1976) 133–156 et **283–284** (1976) 71–85.
[4] L.N. Vaserštein, On the group SL_2 over Dedekind ring of arithmetic type, *Math. U.S.S.R.-Sb* **18**(2) (1972) 321–332.