Journal de Théorie des Nombres
de Bordeaux **12** (2000), 531–570

Digits and continuants in Euclidean algorithms. Ergodic versus Tauberian theorems

par Brigitte VALLEE

À Jacques Martinet, meneur d'hommes et de science

Résumé. Nous faisons ici l'analyse en moyenne des principales quantités qui interviennent dans des algorithmes de type Euclide –quotients partiels (chiffres) et continuants–. L'étude de ces paramètres est en particulier essentielle quand on s'intéresse à une mesure très précise (et très réaliste) de la complexité de ces algorithmes, i.e., la complexité en bits, où l'on compte toutes les opérations sur les bits. Nous développons un cadre général pour une telle analyse, où la complexité moyenne est reliée au comportement analytique dans le plan complexe des homographies utilisées par l'algorithme. Nos méthodes sont fondées sur l'utilisation des opérateurs de transfert, objets de base de la théorie des systèmes dynamiques, que nous adaptons à nos besoins. Nous opérons dans un cadre discret, où les théorèmes Taubériens prennent le relais des théorèmes ergodiques. Ainsi, nous obtenons des résultats nouveaux sur la complexité moyenne –mesurée en bits– de toute une classe d'algorithmes de type Euclide, et ce, dans un cadre unificateur.

Abstract. We obtain new results regarding the precise average–case analysis of the main quantities that intervene in algorithms of a broad Euclidean type. We develop a general framework for the analysis of such algorithms, where the average-case complexity of an algorithm is related to the analytic behaviour in the complex plane of the set of elementary transformations determined by the algorithms. The methods rely on properties of transfer operators suitably adapted from dynamical systems theory and provide a unifying framework for the analysis of the main parameters —digits and continuants— that intervene in an entire class of gcd-like algorithms. We operate a general transfer from the continuous case (Continued Fraction Algorithms) to the discrete case (Euclidean Algorithms), where Ergodic Theorems are replaced by Tauberian Theorems.

Manuscrit reçu le 29 février 2000.

Brigitte VALLÉE
GREYC, UMR 6072
Université de Caen
14032 Caen
France
E-mail : `Brigitte.Vallee@info.unicaen.fr`