Ergodic Theory and Average Case Analysis of Euclid's Algorithm

Hervé Daudé
Université de Caen

March 22, 1993

[summary by Philippe Flajolet]

Abstract

This presentation proposes a transfer principle from the continuous to the discrete in the context of the average case analysis of the Euclidean GCD algorithm. By this principle, it is possible to transfer a central limit theorem on the denominators of convergents associated with continued fraction expansions of real numbers to rational fractions naturally associated to the Euclidean GCD algorithm. There results an estimation of small and large deviation probabilities for the Euclidean algorithm. Ergodic theory permits to place these results in a wider perspective.

Bibliographical data

The history of the analysis of the Euclidean algorithm till about 1980 appears in Knuth's book *"Seminumerical Algorithms"* [7].

The worst case of the algorithm on fractions $\frac{p}{q}$ with p, q bounded by N is about $\log_\varphi N$ (with $\varphi = (1+\sqrt{5})/2$) and is related to Fibonacci numbers, as discovered by Lamé in 1845.

The average case is asymptotic to

$$\frac{12\log 2}{\pi^2}\log N,$$

as was discovered independently by Dixon [3] and Heilbronn [4] near 1970. Asymptotic refinements of the average case formula have been given by Porter and Knuth, see [7].

While Heilbronn's approach is number–theoretic, Dixon's proof is based on properties of continued fraction expansions of real numbers. It had been conjectured by Gauß that the kth iterate in the continued fraction expansion of a random uniform $x \in [0, 1]$ has a distribution that tends to the so–called Gauß law with density

$$\frac{1}{\log 2}\,\frac{1}{1+x}.$$

As Gauß himself said: *"Tam complicatæ evadunt ut nulla spes superesse videatur"*.

Gauß's problem was only solved by Paul Lévy in 1929, with successive refinements introduced by Kuzmin and Wirsing who characterized the speed of convergence (as a decaying exponential), and eventually by Babenko who gave an exact spectral decomposition [1] of the distribution of the kth iterate as an infinite sum of decreasing exponentials.

The existence of a limit distribution can be connected to ergodic theory as was noted after Khinchin's work [6] and part of the talk followed this thread. In this context, Gauß's law is nothing but the invariant measure associated with the continued fraction transformation:

$$T(x) = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor.$$

In another direction, it had been proved by Philipp [10] using probabilistic methods that the logarithm of the denominator of a random $x \in [0,1]$ follows a Gaussian law in the limit. Dixon and Daudé make use of this result by transferring properties of the continuous model of continued fractions to the discrete model of rational fractions that underlies the Euclidean algorithm.

Daudé [2, Chap. 1] establishes in this context two results: one that indicates that the probability of "small deviations" is large enough (this resembles a partial limit density estimate for the Euclidean algorithm), another dual one that the probability of "large deviations" is small. Daudé's thesis also contains corresponding results for the variant of the Euclidean algorithm based on the centered quotient–remainder transformation.

Recently, these results have been made more precise by Hensley [5] who established a central limit theorem for the number of steps of the Euclidean algorithm. Hensley's approach depends on functional properties of an operator $\mathcal{G}_s$, closely associated with continued fractions:

$$\mathcal{G}_s[f](z) = \sum_{n=1}^{\infty} \frac{1}{(n+z)^s} f(\frac{1}{n+z}).$$

The functional analysis approach to these problems itself takes its roots in earlier works of Wirsing [12], Babenko [1] and Mayer [8, 9].

The techniques of the talk prove useful for the average case analysis of a lattice reduction algorithm in dimension 2 also due to Gauss, see [2, Chap. 2] and [11].

Bibliography

[1] Babenko (K. I.). – On a problem of Gauss. *Soviet Mathematical Doklady*, vol. 19, n° 1, 1978, pp. 136–140.

[2] Daudé (Hervé). – *Des fractions continues à la réduction des réseaux: analyse en moyenne.* – PhD thesis, Université de Caen, 1993.

[3] Dixon (J. D.). – The number of steps in the Euclidean algorithm. *Journal of Number Theory*, vol. 2, 1970, pp. 414–422.

[4] Heilbronn (H.). – On the average length of a class of continued fractions. In Turan (Paul) (editor), *Number Theory and Analysis.* pp. 87–96. – New York, 1969.

[5] Hensley (Doug). – The number of steps in the Euclidean algorithm, 1993.

[6] Khinchin (A. I.). – *Continued Fractions.* – Chicago, University of Chicago Press, 1964. A translation of the Rusian original published in 1935.

[7] Knuth (Donald E.). – *The Art of Computer Programming.* – Addison-Wesley, 1981, 2nd edition, volume 2: Seminumerical Algorithms.

[8] Mayer (D.) and Roepstorff (G.). – On the relaxation time of Gauss's continued fraction map. I. The Hilbert space approach. *Journal of Statistical Physics*, vol. 47, n° 1–2, April 1987, pp. 149–171.

[9] Mayer (D.) and Roepstorff (G.). – On the relaxation time of Gauss's continued fraction map. II. The Banach space approach (transfer operator approach). *Journal of Statistical Physics*, vol. 50, n° 1–2, January 1988, pp. 331–344.

[10] Philipp (W.). – Ein zentraler Grenzwertsatz mit Anwendungen auf die Zahlentheorie. *Zeitschrift für Wahrscheinlichkeitstheorie*, vol. 8, 1967, pp. 195–203.

[11] Vallée (Brigitte) and Flajolet (Philippe). – Gauss' reduction algorithm: An average case analysis. In *Proceedings of the 31st Symposium on Foundations of Computer Science.* pp. 830–839. – IEEE Computer Society Press, October 1990.

[12] Wirsing (E.). – On the theorem of Gauss-Kusmin-Lévy and a Frobenius-type theorem for function spaces. *Acta Arithmetica*, vol. 24, 1974, pp. 507–528.