Unified Analysis of Euclidean Algorithms

Brigitte Vallée
Université de Caen

March 29, 1999

[summary by Cyril Banderier]

Abstract

The average behavior of nine algorithms derived from the Euclidean Algorithm is analysed. Some of them are useful in computing the Jacobi symbol. It is shown that these algorithms form two classes: the fast and the slow algorithms ($\Theta(\ln N)$) versus $\Theta(\ln^2 N)$). The author suggests a general method, in which the algorithm and the set of its data are viewed as a dynamical system. The Ruelle operator and functional analysis are key tools. This unified approach gives not only the previously known results for classical Euclidean algorithms but also new results about the binary GCD and Jacobi symbol algorithms. In particular, conjectures due to Brent, Bach and Shallit are solved. The average behavior is linked to the entropy of the dynamical system, thus new universal constants (explicit for classical cases, computed numerically in the other cases) are exhibited.

1. Euclidean Algorithms

A previous talk of Brigitte Vallée (see the summary in the proceedings of year 97/98) was devoted to the complete analysis of the binary GCD algorithm. The summary ended by mentioning the application of Vallée's method to the Jacobi Symbol. The last year has seen a unification of the approaches and the reader will find here the analysis of nine algorithms. These are "flip and reduce" algorithms and are more or less variations of the "classical Euclid algorithm", an algorithm which dates from 300BC and which can also be found in a first-century AD Chinese text (Chiu Chang Suan Shu).

Before the "functional analytic number theoretical dynamical systematic" approach of Vallée, the state of the art was due to Brent [1], Knuth [5], Heilbron [4], Dixon [3], Vardi [10], Bach, Shallit [7].

Vallée and her student, C. Lemée, gave some new results for the analysis of the average complexity of the computation of a fundamental function in number theory: the Jacobi symbol, which allows to determine whether a number is a square in a given modular arithmetic or not.

The Legendre symbol is defined for an odd prime number v as

$$(\frac{u}{v}) = \begin{cases} 0, & \text{if } u \equiv 0 \bmod v; \\ 1, & \text{if } v \text{ is a square modulo } v; \\ -1, & \text{if } v \text{ is not a square mod} v. \end{cases}$$

The Jacobi symbol extends the Legendre symbol and is defined as

$$J(u,v) := \prod_{i \in I} (\frac{u}{v_i})^{e_i} \qquad \text{for } v = \prod_{i \in I} v_i^{e_i} \text{ with odd primes } v_i.$$

Of course one does not need to know the factorisation of v in order to compute $J(u,v)$. Instead, one uses the following formulæ:

$$\begin{array}{rll}
\text{Quadratic reciprocity law:} & J(u,v) = (-1)^{(u-1)(v-1)/4} J(v,u) & \text{for } u, v \text{ odd positive integers,} \\
\text{Modulo law:} & J(v,u) = J(v-bu,u), & \\
\text{Multiplicativity law:} & J(vw,u) = J(v,u)J(w,u), & \\
\text{Special values:} & J(2,v) = (-1)^{(v^2-1)/8}, \qquad J(\epsilon,u) = \epsilon^{(u-1)/2} & \text{for } \epsilon = \pm 1.
\end{array}$$

Then one has several Euclidean-like possible algorithms. We distinguish the nine following cases (name, constraints of the algorithm and an example are given):

Classical with positive remainders
$v = cu + r$, $0 \leq r < u$

$$\tfrac{13}{75} = \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{3+0}}}}$$

Subtractive classical
$v = u + (v - u)$

$$\tfrac{13}{75} = \cfrac{1}{1+1+1+1+1+1 + \cfrac{1}{1 + \cfrac{1}{1+1+1 + \cfrac{1}{1+1+1}}}}$$

Classical with negative remainders
$v = cu - r$
$0 \leq r < u$

$$\tfrac{13}{75} = \cfrac{1}{6 - \cfrac{1}{5 - \cfrac{1}{2 - \cfrac{1}{2+0}}}}$$

Classical with centred remainders
$v = cu + \epsilon r$
$c \geq 2, \epsilon = \pm 1, (c,\epsilon) \neq (2,-1)$
$0 \leq r \leq u/2$

$$\tfrac{13}{75} = \cfrac{1}{6 - \cfrac{1}{4 + \cfrac{1}{3}}}$$

Even CF
$v = cu + \epsilon s$,
c even, $\epsilon = \pm 1$ s odd, $0 < s < u$

$$\tfrac{13}{75} = \cfrac{1}{6 - \cfrac{1}{4 + \cfrac{1}{4-1}}}$$

Odd CF
$v = cu + \epsilon 2^k s$,
c odd, $\epsilon = \pm 1$,
s odd, $k \geq 1, 0 \leq 2^k s < u$

$$\tfrac{13}{75} = \cfrac{1}{5 + \cfrac{2}{3 - \cfrac{2}{5+0}}}$$

Ordinary CF
$v = cu + 2^k s$, $s = 0$ or s odd,
$k \geq 0$,
$0 \leq 2^k s < u$

$$\tfrac{13}{75} = \cfrac{1}{5 + \cfrac{2}{2 + \cfrac{1}{1 + \cfrac{2}{3+0}}}}$$

Centred CF
$v = cu + \epsilon 2^k s$,
$s = 0$ or s odd, $k \geq 0$,
$0 \leq 2^k s < u/2$

$$\tfrac{13}{75} = \cfrac{1}{6 - \cfrac{1}{4 + \cfrac{1}{3+0}}}$$

Binary GCD
$v = au + 2^k r$,
a odd,
$a < 2^k$, $r \leq u$

$$\tfrac{13}{75} = \cfrac{1}{1 + 2 + \cfrac{2^2}{1 + \cfrac{2^2}{1+2^3}}}$$

2. Functional Analytic Number theory

Performing l steps of one of the above algorithms gives a continued fraction of height l and the expression of the rational u/v as

$$\frac{u}{v} = h_1 \circ h_2 \circ \cdots \circ h_l(\alpha) \tag{1}$$

where α is 1 or 0 and where the h_i's are "linear fractional transformations" or LFT ("homographie" in French). Of course the values of a, b, c, d in $h_i = \frac{az+b}{cz+d}$ depend on the algorithms. What is more, the shape of the first and last LFT can be different from the other "intermediate" generic LFT, depending on the initial and stopping conditions of the algorithm.

Introduce the double Dirichlet generating function

$$S(s, w) := \sum_{l \geq 1} \sum_{n > 1} \frac{\nu_n^{[l]}}{n^s} w^l$$

where $\nu_n^{[l]}$ is the number of rationals of Ω (set of valid inputs in [0,1] or [0,1/2], depending on the algorithm) of the form u/n which give a continued fraction of height l. Defining a_n and b_n by

$$S(s, 1) =: \sum_{n>1} \frac{a_n}{n^s} \qquad \text{and} \qquad \frac{\partial}{\partial w} S(s, w)|_{w=1} =: \sum_{n>1} \frac{b_n}{n^s}$$

allows to express S_N, the average number of steps of the algorithm on the rationals u/v of Ω for $u \leq N$, as

$$S_N = \frac{\sum_{n \leq N} b_n}{\sum_{n \leq N} a_n} = \frac{\sum_{n \leq N} \sum_{l \geq 0} l \nu_n^{[l]}}{\sum_{n \leq N} \sum_{l \geq 0} \nu_n^{[l]}}.$$

Thus the average behavior of the algorithm is dictated by the asymptotics of partial sums of coefficients of the function S.

For any Dirichlet series $F(s)$ with nonnegative coefficients a_n converging in $\Re(s) > \sigma > 0$, a theorem of Delange gives

$$\sum_{n \leq N} a_n = \frac{A}{\sigma \Gamma(\gamma + 1)} N^\sigma \ln^\gamma N (1 + o(N)).$$

As for any Tauberian theorem, $F(s)$ has to fulfill some hypotheses (analyticity on $\Re(s) = \sigma$ for $s \neq \sigma$ and there exist A, B analytic at σ such that $F(s) = A(s)(s-\sigma)^{-\gamma-1} + B(s)$). A major part of the the work consists in proving that these properties hold.

Recall that for each algorithm, there are 4 sets of LFT: the single LFT's $\mathcal{K}$, the initial LFT's $\mathcal{I}$, the final LFT's $\mathcal{F}$ and the intermediate LFT's $\mathcal{H}$. Now define the "Ruelle operator" A relative to a set $\mathcal{A}$ of LFT's by

$$A_s(f) = \sum_{h \in \mathcal{A}} \frac{f \circ h}{\mathrm{denom}(h)^s}.$$

The decomposition of an algorithm as a single LFT or as final+sequence(intermediate)+initial LFT's (for short $\mathcal{K} + \mathcal{F}\mathcal{H}^*\mathcal{J}$) leads to $S(s,w) = wK_s(1)(\alpha) + w^2 F_s \circ (I - wH_s)^{-1} \circ J_s(1)(\alpha)$ (where α is defined as in equation 1 and where $\circ$ is the composition over the space of operators). Variations for Markovian cases are possible and lead to the same treatment.

Finally, spectral properties of $I - H_s$ allow to determine $\sigma = 2$ and $\gamma = 1$ or 2 (in some cases, one needs to choose an adequate functional space in order to establish this).

Here is a summary of the average number of steps performed by the nine algorithms:

positive remainders	$\frac{12\ln 2}{\pi^2}\ln N$	$.842\ln N$	Heilbron & Dixon 70
subtractive	$\frac{6}{\pi^2}(\ln N)^2$	$.607(\ln N)^2$	Knuth & Yao 75
negative remainders	$\frac{3}{\pi^2}(\ln N)^2$	$.303(\ln N)^2$	Vardi 92
centred remainders	$\frac{12\ln\phi}{\pi^2}\ln N$	$.585\ln N$	Rieger 80
even	$\frac{2}{\pi^2}(\ln N)^2$	$.202(\ln N)^2$	Vallée & Lemée 98
odd	$A_O\ln N$	$.435\ln N$	Vallée & Lemée 98
ordinary	$A_U\ln N$	$.535\ln N$	Vallée & Lemée 98
centred	$A_C\ln N$	$.430\ln N$	Vallée & Lemée 98
binary GCD	$A_B\ln N$	$.555\ln N$	Vallée 98

The author also makes the link between the constants given here and the entropy of the dynamical system related to the algorithm.

The results presented here are mainly in [9] and in a preprint of Brigitte and her student [6]. Like other preprints of the author, it is available at her home page
`http://www.info.unicaen.fr/~brigitte/Publications/`

Bibliography

[1] Brent (Richard P.). – Analysis of the binary Euclidean algorithm. In *Algorithms and complexity*, pp. 321–355. – Academic Press, New York, 1976. Proceedings of a Symposium held at Carnegie-Mellon University, 1976.

[2] Delange (Hubert). – Généralisation du théorème de Ikehara. *Annales Scientifiques de l'École Normale Supérieure*, vol. 71, n° 3, 1954, pp. 213–242.

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

[4] Heilbronn (H.). – On the average length of a class of finite continued fractions. In *Number Theory and Analysis (Papers in Honor of Edmund Landau)*, pp. 87–96. – Plenum, New York, 1969.

[5] Knuth (Donald E.). – *The Art of Computer Programming.* – Addison-Wesley, 1997, third edition, vol. 2.

[6] Lemée (Charlie) and Vallée (Brigitte). – Analyse des algorithmes du symbole de Jacobi. *GREYC*, 1998.

[7] Shallit (Jeffrey). – Origins of the analysis of the Euclidean algorithm. *Historia Mathematica*, vol. 21, n° 4, 1994, pp. 401–419.

[8] Vallée (Brigitte). – The complete analysis of the binary Euclidean algorithm. In *Proceedings ANTS'98.* – 1998.

[9] Vallée (Brigitte). – A Unifying Framework for the Analysis of a Class of Euclidean Algorithms. In *Proceedings FOCS'99.* – 1999.

[10] Vardi (Ilan). – Dedekind sums have a limiting distribution. *Duke Mathematical Journal*, n° 1, 1993, pp. 1–12.