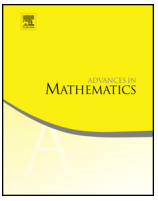
Advances in Mathematics 290 (2016) 73–143

Contents lists available at ScienceDirect

Advances in Mathematics

www.elsevier.com/locate/aim



A rigorous version of R.P. Brent's model for the binary Euclidean algorithm

Ian D. Morris

Department of Mathematics, University of Surrey, Guildford GU2 7XH, United Kingdom

ARTICLE INFO

Article history:
Received 12 September 2014
Received in revised form 8 December 2015
Accepted 9 December 2015
Available online 22 December 2015
Communicated by Kenneth Falconer

MSC:
primary 11A05, 11Y16, 68W40
secondary 11Y60, 37C30, 37H99

Keywords:
Euclidean algorithm
Greatest common divisor
Analysis of algorithms
Transfer operator
Random dynamical system

ABSTRACT

The binary Euclidean algorithm is a modification of the classical Euclidean algorithm for computation of greatest common divisors which avoids ordinary integer division in favour of division by powers of two only. The expectation of the number of steps taken by the binary Euclidean algorithm when applied to pairs of integers of bounded size was first investigated by R.P. Brent in 1976 via a heuristic model of the algorithm as a random dynamical system. Based on numerical investigations of the expectation of the associated Ruelle transfer operator, Brent obtained a conjectural asymptotic expression for the mean number of steps performed by the algorithm when processing pairs of odd integers whose size is bounded by a large integer. In 1998 B. Vallée modified Brent's model via an induction scheme to rigorously prove an asymptotic formula for the average number of steps performed by the algorithm; however, the relationship of this result with Brent's heuristics remains conjectural. In this article we establish previously conjectural properties of Brent's transfer operator, showing directly that it possesses a spectral gap and preserves a unique continuous density. This density is shown to extend holomorphically to the complex right half-plane and to have a logarithmic singularity at zero. By combining these results with methods from classical analytic number theory we prove the correctness of three conjectured formulae for the expected number of steps,

E-mail address: i.morris@surrey.ac.uk.

http://dx.doi.org/10.1016/j.aim.2015.12.008
0001-8708/© 2016 The Author. Published by Elsevier Inc. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

resolving several open questions promoted by D.E. Knuth in *The Art of Computer Programming*.
© 2016 The Author. Published by Elsevier Inc. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

The classical Euclidean algorithm for the computation of the greatest common divisor (GCD) of a pair of natural numbers has been described as the oldest nontrivial algorithm which remains in use to the present day [22, p. 335]. The investigation of the number of division steps required by the Euclidean algorithm dates back at least to the 16th century, when it was observed that pairs of consecutive Fibonacci numbers result in particularly long running times [38]. The mathematically rigorous analysis of the number of division steps began in the mid-19th century with P.-J.-É. Finck's demonstration in [13] that the number of division steps required for the algorithm to process a pair of integers is bounded by a constant multiple of the logarithm of the larger of the two integers; a detailed historical exposition may be found in [39]. Asymptotic expressions for the mean number of division steps required to process a pair of natural numbers (u, v) such that $1 \leq u \leq v \leq n$ were obtained in the 20th century by J.D. Dixon [9] and H. Heilbronn [17] and were subsequently refined by J.W. Porter [36]. In 1994 it was shown by D. Hensley [19] that the distribution of the number of division steps about its mean is asymptotically normal in the limit as $n \to \infty$, and this result has been extended and generalised by V. Baladi and B. Vallée [2,6].

The binary Euclidean algorithm, proposed in 1967 by J. Stein [41] but possibly used in 1st-century China [22, p. 340], is a variant of the Euclidean algorithm which is adapted to the requirements of binary arithmetic, and is one of the fundamental algorithms for the computation of greatest common divisors. In sharp contrast to the classical Euclidean algorithm it is one of the least well-understood algorithms for GCD computation [45, §3]. Early heuristic investigations by R.P. Brent [3] led to a conjectured asymptotic expression for the mean number of steps performed by the binary Euclidean algorithm which remains unproved: using a modification of Brent's model B. Vallée has shown rigorously that the mean number of steps performed by the algorithm grows logarithmically with the size of the input [43], but the relationship of her result to the heuristic formulae given in earlier research remains conjectural. The purpose of this article is to directly transform the heuristic investigations of R.P. Brent into a rigorous argument and to prove the validity of the various conjectured asymptotic expressions for the mean number of steps, resolving a number of open questions promoted by D.E. Knuth in *The Art of Computer Programming* ([21, p. 339] and [22, p. 355]).[1]

[1] *The Art of Computer Programming* uses a scale from 0 to 50 to rank the difficulty of exercises, where 0 denotes triviality and 50 indicates a formidable unsolved research problem. The problems solved in this

Download English Version:

https://daneshyari.com/en/article/6425302

Download Persian Version:

https://daneshyari.com/article/6425302

Daneshyari.com