Complete Analysis of the Binary GCD Algorithm

Brigitte Vallée
Université de Caen

April 27, 1998

[summary by Cyril Banderier]

1. Introduction

The analysis of the *classical* Euclidean algorithm has been performed by Heilbronn [4] and Dixon [3], using different approaches. For a random pair of rational numbers, the average number of divisions is

$$D_n \sim \frac{12 \log 2}{\pi^2} \log n.$$

Here, we will analyse the *binary* Euclidean algorithm, which uses only subtractions and right binary shifts. This "binary GCD algorithm" takes as input a pair of odd integers (u, v) from the set $\Omega = \{(u, v) \text{ odd}, 0 < u \leq v\}$. Then the GCD is recursively defined by

$$\begin{cases} \gcd(u, v) = \gcd\left(\frac{v-u}{2^{\mathrm{Val}_2(v-u)}}, v\right) \\ \gcd(u, v) = \gcd(v, u) \end{cases}$$

where $\mathrm{Val}_2(n)$ is the greatest integer b such 2^b divides n, i.e., the dyadic valuation of n. The corresponding binary GCD algorithm is as follows:

while $u \neq v$ **do**
  while $u < v$ **do**
    $b := \mathrm{Val}_2(v - u)$;
    $v := (v - u)/2^b$;
  end;
  exchange u **and** v;
end;
return u.

Example. If the input is $(u, v) := (7, 61)$ then $b := \mathrm{Val}_2(61 - 7) = 1$. Thus $v := 54/2^1 = 27$, and the algorithm continues because $u < v$. Now $b := \mathrm{Val}_2(27 - 7) = 2$. Thus $v := 20/2^2 = 5$. Now the algorithm restarts with $(u, v) := (5, 7)$. It leads to $v := (7 - 5)/2^1 = 1$ and therefore one restarts with $(u, v) := (1, 5)$ which leads to $v = 1 = u$ so the algorithm stops and returns u, namely 1 (as expected since 7 and 61 are coprime). One can write:

$$\frac{7}{61} = \cfrac{1}{3 + \cfrac{2^3}{1 + \cfrac{2^1}{1 + 2^2}}}.$$

In general, for each "inner while loop", one has

$$x_i = \frac{1}{a_i + 2^{k_i} x_{i+1}}$$

where $x_i := u/v$ (with (u,v) as in the beginning of the loop), $x_{i+1} := u/v$ (with (u,v) as after the exchange), where $a_i := 1 + 2^{b_1} + 2^{b_1+b_2} + \cdots + 2^{b_1+\cdots+b_{l-1}}$ and $k_i := b_1 + \cdots + b_{l-1} + b_l$ (the sum of all the b's obtained during the i-th inner while loop). The algorithm thus produces the following binary continued fraction expansion

$$\frac{u}{v} = \cfrac{1}{a_1 + \cfrac{2^{k_1}}{\ddots + \cfrac{2^{k_{r-1}}}{a_r + 2^{k_r}}}}.$$

Three interesting parameters are:

- r, the depth of the continued fraction or equivalently the number of outer loops performed;
- $\sum_{i=1}^{r} \nu(a_i)$, the number of subtractions (where $\nu(w)$ is the number of 1's in the binary expansion of the integer w);
- $\sum_{i=1}^{r} k_i$, number of rights shifts performed or equivalently inner loop executions.

Their average values on the set $\Omega_n = \{(u,v)\,\text{odd}, 0 < u \le v \le n\}$ are respectively noted E_n, P_n and S_n. Note that E_n is also the average number of exchanges in the algorithm, and that P_n is the average number of operations that are necessary to obtain the expansion.

2. A Ruelle Operator for a Tauberian Theorem

In order to establish that these three parameters have averages that are asymptotic to $\log n$, we introduce the following Ruelle operator:

$$V_s[f](x) := \sum_{k\ge 1} \sum_{\substack{a \text{ odd} \\ 1 \le a \le 2^k}} \frac{1}{(a+2^k x)^s} f\left(\frac{1}{a+2^k x}\right).$$

The average E_n is easily expressed in term of V_s, with the help of the following definitions:

$$F(s) := (\mathrm{Id} - V_s)^{-1}[\mathrm{Id}](1), \quad G(s) := (\mathrm{Id} - V_s)^{-2} \circ V_s[\mathrm{Id}](1), \qquad \tilde{\zeta}(s) := \sum_{k \text{ odd}} \frac{1}{k^s} = \left(1 - \frac{1}{2^s}\right)\zeta(s).$$

Proposition 1. *E_n is a ratio of partial sums of the two Dirichlet series $\tilde{\zeta}(s)F(s)$ and $\tilde{\zeta}(s)G(s)$.*

Proof. Let $\Omega^{[l]}$ be the subset of Ω for which the algorithm performs exactly l exchanges. Then,

$$V_s^l[f](1) = \frac{1}{\tilde{\zeta}(s)} \sum_{(u,v)\in\Omega^{[l]}} \frac{1}{v^s} f\left(\frac{u}{v}\right).$$

Summing over all the possible heights ($l \ge 0$) yields:

$$(\mathrm{Id} - wV_s)^{-1}[f](1) = \sum_{l \ge 0} w^l V_s^l[f](1) = \frac{1}{\tilde{\zeta}(s)} \sum_{(u,v)\in\Omega^{[l]}} \frac{1}{v^s} f\left(\frac{u}{v}\right).$$

Differentiating with respect to w, and then choosing $f = 1$ and $w = 1$ yields

$$E_n = \frac{1}{|\Omega_n|} \sum_{l\ge 0} l |\Omega_n^{[l]}| = \frac{\sum_{l\ge 0} l \sum_{k \le n} v_k^{[l]}}{\sum_{l \ge 0} \sum_{k\le n} v_k^{[l]}}.$$

The proof is completed by observing that

$$F(s) = \frac{1}{\tilde{\zeta}(s)} \sum_{k\geq 1} \frac{1}{v^s} \sum_{l\geq 0} v_k^{[l]}, \qquad G(s) = \frac{1}{\tilde{\zeta}(s)} \sum_{k\geq 1} \frac{1}{v^s} \sum_{l\geq 0} l v_k^{[l]}.$$

□

The key is now to prove that the following theorem may be used:

Theorem 1 (Tauberian theorem). *If $F(s)$ is a Dirichlet series with non-negative coefficients that is convergent for $\Re(s) > \sigma > 0$ and if*

1. *F is analytic on the line $\Re(s) = \sigma$ except at $s = \sigma$;*
2. *$F(s) = \frac{A(s)}{(s-\sigma)^{\gamma+1}} + C(s)$ where A, C are analytic at σ (with $A(\sigma) \neq 0$);*

then one has, as $n \to \infty$,

$$\sum_{k\leq n} a_k = \frac{A(\sigma)}{\sigma\Gamma(\gamma+1)} n^\sigma \log^\gamma n(1+\epsilon(n)),$$

where $\epsilon(n) \to 0$.

Proof. See Delange [2]. □

Lemma 1. *The Tauberian theorem applies to F with $\sigma = 2$ and $\gamma = 0$.*

Proof. Indeed

$$F(s) := (\mathrm{Id} - V_s)^{-1}[\mathrm{Id}](1) = 1 + \frac{1}{2\tilde{\zeta}(s)} \sum_{v \text{ odd}} \frac{v-1}{v^s} = \frac{1}{2}\left(\frac{\tilde{\zeta}(s-1)}{\tilde{\zeta}(s)} + 1\right).$$

The last member of the equality clearly satisfies the conditions of the Tauberian theorem, and the same holds for $\tilde{\zeta}F$ with $\sigma = 2$ and $\gamma = 0$. □

Lemma 2. *The Tauberian theorem applies to G with $\sigma = 2$ and $\gamma = 1$.*

Proof. Here lies the complex part of Brigitte Vallée's proof. It is impossible to conclude as quickly as in lemma 1, indeed, this time we need to find an appropriate functional space on which V_s is a compact operator. A mixture of various functional analysis theorems (Fejer-Riesz' inequality, Gabriel's inequality, Krasnoselsky's theorem and other works by Shapiro and Grothendieck) show that it is the case on the Hardy space $H^2(D)$, where D is an open disk containing $]0,1]$. This leads to the fact that for $s > 3/2$, V_s has a unique positive dominant eigenvalue, equal to 1 when $s = 2$. In addition V_s has a spectral radius < 1 on $\Re(s) \geq 2, s \neq 2$. Thus $(\mathrm{Id} - V_s)^{-1}$ is regular on the domain D and condition 1 of the Tauberian theorem is fulfilled. Condition 2 is proved by means of perturbation theory applied to $V_s = P_s + N_s$ (P_s is the projection of V_s on the dominant eigensubspace), in a neighbourhood of $s = 2$. See [7] for a detailed proof. □

This implies the following fundamental result:

Theorem 2. *The average number of exchanges of the binary Euclidean algorithm on Ω_n is*

$$E_n \sim \frac{2}{\pi^2 f_2(1)} \log n,$$

where f_2 is the fixed point of the operator V_2 that is normalised by $\int_0^1 f_2(t)dt = 1$.

3. The Other Two Parameters

In order to study the other two parameters (total number of subtractions, total number of shifts) one still uses the Tauberian theorem but with a more intricate Ruelle operator, see Vallée [7]. This leads to the following two results.

Theorem 3. *The average number of total iterations is*

$$P_n \sim A \log n \qquad \text{with} \quad A := \frac{2}{\pi^2 f_2(1)} \sum_{a\ odd} \frac{1}{2^{k_a}} F_2\left(\frac{1}{a}\right)$$

where f_2 is defined as above, $F_2(x) := \int_0^x f_2(t)dt$, $F_2(1) = 1$ (where k_a is the integer part of $\log_2 a$*).*

Theorem 4. *The average number of the sum of exponents of 2 used in the numerators of the binary continued fraction expansions, i.e., average total number of right shifts is*

$$S_n \sim \frac{2}{\pi^2 f_2(1)} \left(2 \sum_{a\ odd} \frac{1}{2^{k_a}} F_2\left(\frac{1}{a}\right)\right) \log n.$$

4. All Roads Lead to Rome

In Brent's paper [1], one can find a different approach which suggests that

$$P_n \sim \frac{1}{M} \log n \qquad \text{where} \quad M = \log 2 - \frac{1}{2} \int_0^1 \log(1-x) g_2(x) dx$$

and where g_2 is the fixed point (and normalised as f_2) of

$$B_2[f](x) := \sum_{b \geq 1} \left(\frac{1}{1+2^b x}\right)^2 f\left(\frac{1}{1+2^b x}\right) + \sum_{b \geq 1} \left(\frac{1}{x+2^b}\right)^2 f\left(\frac{x}{x+2^b}\right).$$

Unfortunately, this approach is based on a heuristic hypothesis (exercise 36, section 4.5.2, rated HM49 by Knuth in [5]). Brigitte Vallée explored this approach with a Brent operator B_s, without heuristic arguments but providing a spectral conjecture holds, this leads to the following result:

$$P_n \sim B \log n \qquad \text{where} \quad B := \frac{4}{\pi^2 g_2(1)}.$$

The miracle holds and, after numerical experiments, $A = \frac{1}{M} = B = 1.0185\ldots$. But nobody has proved these equalities. We can also note that a similar method was used by Brigitte Vallée and one of her students to analyse the Jacobi symbol algorithm [6]. Finally, the binary Euclidian algorithm is only a slight variation on one of the oldest known algorithms but there is still some unknown territories in its "complete" analysis!

References

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