Euclidean algorithms and dynamical systems

V. Berthé

IRIF-CNRS-Université Paris Cité
Euclid’s algorithm

We start with two nonnegative integers $u_0$ and $u_1$

\[
\begin{align*}
    u_0 &= u_1 \left\lfloor \frac{u_0}{u_1} \right\rfloor + u_2 \\
    u_1 &= u_2 \left\lfloor \frac{u_1}{u_2} \right\rfloor + u_3 \\
    &\vdots \\
    u_{m-1} &= u_m \left\lfloor \frac{u_{m-1}}{u_m} \right\rfloor + u_{m+1} \\
    u_{m+1} &= \gcd(u_0, u_1) \\
    u_{m+2} &= 0
\end{align*}
\]

One subtracts the smallest number from the largest as much as we can.

The oldest nontrivial algorithm that has survived to the present day

[Knuth]
The advent of high-speed computing machines, which are capable of carrying out algorithms so faithfully, has led to intensive studies of the properties of algorithms, opening up a fertile field for mathematical investigations. Every reasonable algorithm suggests interesting questions of a ‘pure mathematical’ nature; and the answers to these questions sometimes lead to useful applications, thereby adding a little vigor to the subject without spoiling its beauty. [Knuth]

[Origins of the Analysis of the Euclidean Algorithm-Shallit]
Analysis of Euclid’s algorithm

- What is the expected number of steps?
- What is the worst/mean behaviour?
Analysis of Euclid’s algorithm

- What is the expected number of steps?
- What is the worst/mean behaviour?

- Dynamical systems and Perron-Frobenius machinery
- Euclid’s algorithm becomes in its continuous version the Gauss transformation

\[ T : [0, 1] \rightarrow [0, 1], \ x \mapsto \{1/x\} \]

- Rational trajectories behave like generic trajectories for the Gauss transformation
Analysis of algorithms

- Analysis of algorithms [Knuth’63]
  probabilistic, combinatorial, and analytic methods

- Analytic combinatorics [Flajolet-Sedgewick]
  generating functions and complex analysis, analysis of the singularities

- Dynamical analysis of algorithms [Vallée]
  Transfer operators \( \rightsquigarrow \) Generating functions of Dirichlet type
Euclid algorithm and continued fractions

We start with two coprime integers \( u_0 \) and \( u_1 \)

\[
\begin{align*}
  u_0 &= u_1 a_1 + u_2 \\
  & \quad \cdot \\
  u_{m-1} &= u_m a_m + u_{m+1} \\
  u_m &= u_{m+1} a_{m+1} + 0 \\
  u_{m+1} &= 1 = \gcd(u_0, u_1)
\end{align*}
\]
Euclid algorithm and continued fractions

We start with two coprime integers $u_0$ and $u_1$

$$u_0 = u_1 a_1 + u_2$$

$$\vdots$$

$$u_{m-1} = u_m a_m + u_{m+1}$$

$$u_m = u_{m+1} a_{m+1} + 0$$

$$u_{m+1} = 1 = \gcd(u_0, u_1)$$

$$\frac{u_1}{u_0} = \frac{1}{a_1 + \frac{u_2}{u_1}}$$

$$u_1/u_0 = \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_m + \frac{1}{a_{m+1}}}}}}$$
Matricial description

We start with two positive real numbers \((x_0, x_1)\) with \(x_0 > x_1\)
We divide the largest entry by the smallest and we continue

\[
x_0 = \lfloor x_0 / x_1 \rfloor x_1 + x_2 \quad \quad a_1 := \lfloor x_0 / x_1 \rfloor
\]

\[
\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \ldots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix}
\]
Matricial description

We start with two positive real numbers \((x_0, x_1)\) with \(x_0 > x_1\). We divide the largest entry by the smallest and we continue

\[
x_0 = \lfloor x_0/x_1 \rfloor x_1 + x_2 \quad \text{and} \quad a_1 := \lfloor x_0/x_1 \rfloor
\]

\[
\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix}
\]

Let \(\alpha := x_1/x_0\). One has \(\alpha \in [0, 1]\).

Let \(T(\alpha) = 1/\alpha - \lfloor 1/\alpha \rfloor\).

\[
\begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \alpha \begin{pmatrix} \lfloor 1/\alpha \rfloor & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ T(\alpha) \end{pmatrix}
\]

\[
\begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \alpha \cdots T^{n-1}(\alpha) \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ T^n(\alpha) \end{pmatrix}
\]

Number of steps \(\sim\) size of a product of matrices \(\sim\) first Lyapunov exponent
Matricial description

We start with two positive real numbers \((x_0, x_1)\) with \(x_0 > x_1\).
We divide the largest entry by the smallest and we continue

\[
x_0 = \lfloor x_0/x_1 \rfloor x_1 + x_2 \\
a_1 := \lfloor x_0/x_1 \rfloor
\]

\[
\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix}
\]

We normalize \(\alpha := x_1/x_0\) and we set

\[
M_n := \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 \\ \alpha \end{pmatrix} \in \bigcap_n M_1 \cdots M_n \mathbb{R}_+^2
\]

\[
M_1 \cdots M_n = \begin{pmatrix} q_n & q_{n-1} \\ p_n & p_{n-1} \end{pmatrix} \sim \text{a sequence of lattice bases for } \mathbb{Z}^2
Number of steps $\ell(u,v)$

$\ell(u,v)$: number of steps in Euclid algorithm $0 < v < u$

- **Worst case**

  $\ell(u,v) = O(\log v)$  \(\leq 5 \log_{10} v\), Lamé 1844

- **Mean case**

  $0 < v < u \leq N \quad \gcd(u,v) = 1$

  $$\mathbb{E}_N[\ell] = \frac{12 \log 2}{\pi^2} \cdot \log N + \eta + O(N^{-\gamma})$$

Asymptotically normal distribution

[Knuth, Heilbronn’69, Dixon’70, Porter’75, Hensley’94, Baladi-Vallée’05…]
Consider the Gauss map

\[ T : [0, 1] \rightarrow [0, 1], \ x \mapsto \{ 1/x \} \]

\[ x_1 = T(x) = \{ 1/x \} = \frac{1}{x} - \left[ \frac{1}{x} \right] = \frac{1}{x} - a_1 \]

\[ x = \frac{1}{a_1 + x_1} \]

\[ a_n = \left[ \frac{1}{T^{n-1}x} \right] \]

\[ x = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} \]
Continued fractions and dynamical systems

Consider the Gauss map

\[ T : [0, 1] \rightarrow [0, 1], \quad x \mapsto \{1/x\} \]

\[ T(x) = \{1/x\} = \frac{1}{x} - \left[ \frac{1}{x} \right] = \frac{1}{x} - a_1 \]

\[ \frac{1}{k+1} < x \leq \frac{1}{k} \Rightarrow a_1 = k \]
Consider the Gauss map

\[ T : [0, 1] \rightarrow [0, 1], \ x \mapsto \{1/x\} \]

- For a.e. \( x \in [0, 1] \)
  \[
  \lim_{n} \frac{\log q_n}{n} = \frac{\pi^2}{12 \log 2}
  \]

- For a.e. \( x \) and for \( a \geq 1 \)
  \[
  \lim_{N \rightarrow \infty} \frac{1}{N} \{k \leq N; \ a_k = a\} = \frac{1}{\log 2} \log \left(\frac{(a + 1)^2}{a(a + 2)}\right)
  \]
Think of \( f \) as a density function

\[
\mathcal{L}f(x) = \sum_{y : T(y) = x} \frac{1}{|T'(y)|} f(y) = \sum_{a \geq 1} \left( \frac{1}{a+x} \right)^2 f \left( \frac{1}{a+x} \right)
\]
On the iterates of Perron–Frobenius’ operator

Think of $f$ as a density function

$$\mathcal{L}f(x) = \sum_{y : T(y) = x} \frac{1}{|T'(y)|} f(y) = \sum_{a \geq 1} \left( \frac{1}{a + x} \right)^2 f \left( \frac{1}{a + x} \right)$$

Let $x = [0; a_1, a_2, \cdots]$. 

$$\mathcal{L}^k f(x) = \sum_{a_1, \cdots, a_k} \frac{1}{(q_{k-1}x + q_k)^2} f \left( \frac{p_{k-1}x + p_k}{q_{k-1}x + q_k} \right)$$

Perron–Frobenius On a suitable functional space, there exists $\rho < 1$ such that

$$\mathcal{L}^k f(x) = \frac{1}{\log 2} \frac{1}{1 + x} \int_0^1 f(x) \, dx + O(\rho^k \| f \|)$$
On the iterates of Perron–Frobenius’ operator

Think of $f$ as a density function

$$
\mathcal{L} f(x) = \sum_{y : T(y) = x} \frac{1}{|T'(y)|} f(y) = \sum_{a \geq 1} \left( \frac{1}{a + x} \right)^2 f \left( \frac{1}{a + x} \right)
$$

Ruelle operator

$$
\mathcal{L}_s f(x) = \sum_{h \in \mathcal{H}} h'(x)^s \cdot f \circ h(x) \quad s \in \mathbb{C}
$$

Involving additive costs

$$
\mathcal{L}_{s,w} f(x) = \sum_{h \in \mathcal{H}} h'(x)^s \cdot e^{w c(h)} \cdot f \circ h(x)
$$

The parameter $w$ will be used for the study of probabilistic limit theorems and the parameter $s$ plays a role in the study of Hausdorff dimensions.
We consider a positive real number $\alpha$.

One looks for sequences of rational numbers $(p_n/q_n)_n$ that satisfies

$$\lim p_n/q_n = \alpha$$

Continued fractions allow to do it with exponential speed

$$|\alpha - p_n/q_n| \leq \frac{1}{q_n^2}$$
Multidimensional continued fractions

If we start with two parameters \((\alpha, \beta)\), one looks for two sequences of rational numbers \((p_n/q_n)\) and \((r_n/q_n)\) with the same denominator that satisfy

\[
\lim p_n/q_n = \alpha \quad \lim r_n/q_n = \beta
\]

Expected speed \(3/2\)

\[
|\alpha - p_n/q_n| \leq 1/q_n^{3/2} \quad |\beta - r_n/q_n| \leq 1/q_n^{3/2}
\]
Dirichlet’s bound and exponential convergence

Dirichlet’s theorem We are given a $d$-dimensional real vector $\alpha = (\alpha_1, \cdots, \alpha_d) \in [0, 1]^d$. For any positive integer $N$, there exist integers $p_1, \ldots, p_d, q$ with

$$1 \leq q \leq N$$

such that

$$|p_i - q\alpha_i| < \frac{1}{N^{1/d}} \quad i = 1, 2, \cdots, d$$
Dirichlet’s bound and exponential convergence

Dirichlet’s theorem  We are given a $d$-dimensional real vector $\alpha = (\alpha_1, \cdots, \alpha_d) \in [0, 1]^d$. For any positive integer $N$, there exist integers $p_1, \ldots, p_d, q$ with

$$1 \leq q \leq N$$

such that

$$|p_i - q\alpha_i| < \frac{1}{N^{1/d}} \leq \frac{1}{q^{1/d}} \quad i = 1, 2, \cdots, d$$

Dirichlet’s bound $1 + 1/d$

$$\left| \frac{p_i}{q} - \alpha_i \right| \leq \frac{1}{q^{1+\frac{1}{d}}}$$
Jacobi-Perron algorithm (1868-1907)

Consider the Jacobi-Perron algorithm. Its projective version is defined on the unit square \([0, 1]^2\) by

\[
(x, y) \mapsto \left( \frac{y}{x} - \left\lfloor \frac{y}{x} \right\rfloor, \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor \right) = \left( \left\{ \frac{y}{x} \right\}, \left\{ \frac{1}{x} \right\} \right).
\]

With \(x = b/a, y = c/a\), its linear version is defined on the positive cone \(\{ (a, b, c) \in \mathbb{R}^3 | 0 < b, c < a \}\) by

\[
(a, b, c) \mapsto (a_1, b_1, c_1) = (b, c - \lfloor c/b \rfloor b, a - \lfloor a/b \rfloor b).
\]

Set \(C = \lfloor c/b \rfloor, A = \lfloor a/b \rfloor\). One has

\[
\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} A & 0 & 1 \\ 1 & 0 & 0 \\ C & 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 \\ b_1 \\ c_1 \end{pmatrix} = \begin{pmatrix} A & 0 & 1 \\ 1 & 0 & 0 \\ C & 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ c - Cb \\ a - Ab \end{pmatrix}.
\]
Theorem of Perron–Frobenius type

One considers an infinite product of matrices

$$E_1 \cdots E_k \cdots$$

with entries in $\mathbb{N}$. One assumes that there exists a matrix $B$ with strictly positive entries s.t. there exist $i_1 < j_1 < \cdots < i_k < j_k$ s.t.

$$B = E_{i_1} \cdots E_{j_1}, \cdots, B = E_{i_k} \cdots E_{j_k}, \cdots.$$

Then, the intersection of the cones

$$\cap_k E_1 \cdots E_k(\mathbb{R}_+^n)$$

is unidimensional [Furstenberg]

$$\sim \text{ Convergence}$$
Convergence for simultaneous approximations

\[ M_1 \cdots M_n = \begin{pmatrix} q_1^{(n)} & \cdots & q_{d+1}^{(n)} \\ p_{1,1}^{(n)} & \cdots & p_{1,d+1}^{(n)} \\ \vdots & \ddots & \vdots \\ p_{d,1}^{(n)} & \cdots & p_{d,d+1}^{(n)} \end{pmatrix} \sim \begin{pmatrix} p_{1,j}^{(n)} \\ q_{j}^{(n)} \\ \vdots \\ p_{d,j}^{(n)} \\ q_{j}^{(n)} \end{pmatrix} \]

Weak convergence Convergence in angle

\[ \lim_{n \to +\infty} \begin{pmatrix} p_{1,j}^{(n)} \\ q_{j}^{(n)} \\ \vdots \\ p_{d,j}^{(n)} \\ q_{j}^{(n)} \end{pmatrix} = (\alpha_1, \cdots, \alpha_d) \]

Strong convergence Convergence in distance

\[ \lim_{n \to +\infty} |q_{j}^{(n)} \alpha_i - p_{i,j}^{(n)}| = 0 \text{ for all } i, j \]
Convergence of Jacobi-Perron algorithm

Theorem [Broise-Guivarc’h’99] There exists $\delta > 0$ s.t. for almost every $(\alpha, \beta)$

$$|\alpha - p_n/q_n| < \frac{1}{q_n^{1+\delta}}, \quad |\beta - r_n/q_n| < \frac{1}{q_n^{1+\delta}}$$

where $p_n, q_n, r_n$ are produced by either by Jacobi-Perron algorithm

What is the dependence of $\delta$ with respect to the number of parameters?
Lyapunov exponents

We consider a MCF algorithm given by a piecewise constant transformation

\[ A : [0, 1]^d \to \text{GL}(d + 1, \mathbb{Z}) \]

with its associated transformation \(([0, 1]^d, T_A, \nu)\). We assume \(\nu\) ergodic. Let

\[ A^{(n)}(u) = A(u)A(T_A u) \cdots A(T_A^{n-1} u). \]

We assume \(\log^+ ||A(x)||\) is \(\nu\)-integrable (\(\log^+(a) = \max\{\log a, 0\}\) for \(a > 0\)).

Then by the Oseledeets Theorem the following Lyapunov exponents \(\lambda_k, 1 \leq k \leq d+1\), exist

\[ \lambda_1 + \cdots + \lambda_k = \lim_{n \to \infty} \frac{1}{n} \log \| \wedge^k A^{(n)}(u) \| \quad \text{for } \nu\text{-a.e. } u \in \Delta. \]
Lyapunov exponents

\[ A_n(x) = \begin{pmatrix} q_n & q_{n-1} \\ p_n & p_{n-1} \end{pmatrix} \]

**Theorem** For a.e. \( x \),

\[
\lim_{n \to \infty} \frac{1}{n} \log q_n = \frac{\pi^2}{12 \log 2} = 1.18 \ldots = \lambda_1
\]

\( \lambda_1 \) is the *first Lyapunov exponent*

*First Lyapunov exponent* = “log largest eigenvalue” \( \sim \) size of the matrices/convergents \( A_n(x) \sim q_n(x) \sim e^{\lambda_1 n} \)

Number of steps in Euclid’s algorithm = size / log eigenvalue

\[
\log \frac{N}{\lambda_1}
\]

*Second Lyapunov exponent* = "log of the second eigenvalue" \( \sim \) measures the distance between column vectors
Lyapunov exponents

First Lyapunov exponent $\lambda_1 = \log$ largest eigenvalue $\sim$ size of the matrices/convergents $M^{(n)}(\alpha) \sim q_i^n(\alpha) \sim e^{\lambda_1 n}$

Second Lyapunov exponent $\lambda_2 = $ "log of the second eigenvalue" $\sim$ measures the distance between column vectors

$$M^{(n)}(\alpha) = \begin{pmatrix} q_1^{(n)} & \cdots & q_{d+1}^{(n)} \\ p_1^{(n)} & \cdots & p_{1,d+1}^{(n)} \\ \vdots & \ddots & \vdots \\ p_{d,1}^{(n)} & \cdots & p_{d,d+1}^{(n)} \end{pmatrix}$$
Lyapunov exponents

First Lyapunov exponent = \( \log \text{ largest eigenvalue} \sim \text{ size of the matrices/convergents} \ M^{(n)}(\alpha) \sim q_i^n(\alpha) \sim e^{\lambda_1 n} \)

Second Lyapunov exponent = "log of the second eigenvalue" \( \sim \) measures the distance between column vectors

\[ M^{(n)}(\alpha) = \begin{pmatrix} q_1^{(n)} & \cdots & q_{d+1}^{(n)} \\ p_{1,1}^{(n)} & \cdots & p_{1,d+1}^{(n)} \\ \vdots & & \vdots \\ p_{d,1}^{(n)} & \cdots & p_{d,d+1}^{(n)} \end{pmatrix} \]

\[ \lambda_1 \leftrightarrow \log \| M^{(n)} \| \]

\[ \lambda_1 + \lambda_2 \leftrightarrow \log \| \wedge^2 M^{(n)} \| \leftrightarrow \log \| c_i^{(n)} \wedge c_j^{(n)} \| \]

\[ \lambda_2 \text{ distance between column vectors} \]

Dirichlet’s bound \( 1 + 1/d \) vs. \( 1 - \lambda_2/\lambda_1 \)
Higher-dimensional case

Numerical experiments indicate that classical multidimensional continued fraction algorithms seem to cease to be strongly convergent for high dimensions. The only exception seems to be the Arnoux-Rauzy algorithm which, however, is defined only on a set of measure zero [B.-Steiner-Thuswaldner]
Higher-dimensional case

Numerical experiments indicate that classical multidimensional continued fraction algorithms seem to cease to be strongly convergent for high dimensions. The only exception seems to be the Arnoux-Rauzy algorithm which, however, is defined only on a set of measure zero [B.-Steiner-Thuswaldner]

<table>
<thead>
<tr>
<th>$d$</th>
<th>$\lambda_2(A_J)$</th>
<th>$1 - \frac{\lambda_2(A_J)}{\lambda_1(A_J)}$</th>
<th>$d$</th>
<th>$\lambda_2(A_J)$</th>
<th>$1 - \frac{\lambda_2(A_J)}{\lambda_1(A_J)}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>−0.44841</td>
<td>1.3735</td>
<td>7</td>
<td>−0.02819</td>
<td>1.0243</td>
</tr>
<tr>
<td>3</td>
<td>−0.22788</td>
<td>1.1922</td>
<td>8</td>
<td>−0.01470</td>
<td>1.0127</td>
</tr>
<tr>
<td>4</td>
<td>−0.13062</td>
<td>1.1114</td>
<td>9</td>
<td>−0.00505</td>
<td>1.0044</td>
</tr>
<tr>
<td>5</td>
<td>−0.07880</td>
<td>1.0676</td>
<td>10</td>
<td>+0.00217</td>
<td>0.9981</td>
</tr>
<tr>
<td>6</td>
<td>−0.04798</td>
<td>1.0413</td>
<td>11</td>
<td>+0.00776</td>
<td>0.9933</td>
</tr>
</tbody>
</table>

Table: Heuristically estimated values for the second Lyapunov exponent and the uniform approximation exponent of the Jacobi–Perron Algorithm
Let $GL(n, \mathbb{Z})$ stand for the set of matrices with integer entries and determinant $\pm 1$.

**Theorem [Duke-Rudnick-Sarnak]** One has

$$\{ M \in GL(n, \mathbb{Z}), |m_{ij}| \leq T \} \sim c_n T^{n^2-n}$$

How to generate “random matrices” in $GL_n(\mathbb{Z})$?
How does LLL produce good approximations?

Let

\[ M_t := \begin{pmatrix} 1 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & \cdots & 0 & -\alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -\alpha_d \\ 0 & \cdots & \cdots & 0 & t \end{pmatrix} \]
How does LLL produce good approximations?

Let

\[ M_t := \begin{pmatrix}
1 & 0 & \cdots & 0 & -\alpha_1 \\
0 & 1 & \cdots & 0 & -\alpha_2 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & -\alpha_d \\
0 & \cdots & \cdots & 0 & t
\end{pmatrix} \]

LLL produces in polynomial time a vector \( b_1 \) such that

\[ ||b_1|| \leq 2^{d/4} \det(M_t)^{1/d+1} = 2^{d/4} t^{1/d+1} \]

One has

\[ b_1 = (p_1 - q\alpha_1)e_1 + \cdots + (p_d - q\alpha_d e_d) + qte_{d+1} \]

\[ \forall i, \quad |p_i - \alpha_i q| \leq 2^{d/4} t^{1/d+1} \quad \text{and} \quad qt \leq 2^{d/4} t^{1/d+1} \]

\[ \sim \forall i, \quad |p_i - \alpha_i q| \leq 2^{(d+1)/4} 1/q^{1/d} \]