Euclide et Fibonacci

Jean-François Burnol
(v1) 31 mars 2011, (v2) 23 novembre 2017

1 Euclide et matrices 2×2

L'algorithme d'Euclide traditionnel calcule $(a\,,b)$ pour $a, b > 0$. [1]

Posons soigneusement les notations : $r_0 = a$, $r_1 = b$, $a = q_1 b + r_2$, $b = q_2 r_2 + r_3$, $r_2 = q_3 r_3 + r_4$, ... La première étape fait la division euclidienne de a par b. Le quotient est q_1, le reste $r_2 < r_1 = b$. [2] La deuxième étape a un quotient $q_2 \geqslant 1$, un reste $r_3 < r_2$. La n^e étape est avec un quotient q_n et un reste $r_{n+1} < r_n$. Les restes sont tous positifs ou nuls, et même strictement positifs sauf le dernier. Les quotients sont tous au moins égaux à 1, sauf le premier qui est nul si $a < b$, c'est-à-dire si a et b ne « sont pas dans le bon ordre ».

[A] $\quad r_{n-1} = q_n r_n + r_{n+1}\,, \quad 0 \leqslant r_{n+1} < r_n \qquad (n^e \text{ étape})$

La suite des restes est strictement décroissante à partir de $n = 1 : r_1 > r_2 > \ldots$. L'algorithme s'arrête lorsque r_{n+1} est nul. On dit qu'il y a eu alors $N = n$ étapes.

$$r_{N-1} = q_N r_N, \quad r_N = \mathrm{PGCD}(a, b)$$

Par exemple, pour calculer $(10\,,5)$ j'ai besoin d'une étape : $10 = 2 \times 5 + 0$, $N = 1$. Pour calculer $(11\,,5)$ j'ai besoin de deux étapes : $11 = 2 \times 5 + 1$, $5 = 5 \times 1 + 0$, $N = 2$. Bien sûr dans la pratique on est tenté de dire qu'on a fini dès la première étape. Mais pour le théoricien modélisateur, il ne faut pas s'autoriser ce raccourci. Non, encore lui faut-il faire la division par 1 pour s'assurer que le reste est 0. Imaginez-le comme un comptable très pointilleux. Sinon, lui et nous allons nous embrouiller dans le décompte du nombre d'étapes. Le PGCD est le dernier reste non nul. C'est r_N lorsqu'il y a eu N étape. Par exemple si b divise a, il y a 1 étape, et le PGCD est $(a\,,b) = b = r_1$. Si $a = b + 1$, il y a 2 étapes, [3] et $(a\,,b) = 1 = r_2$.

Nous allons associer à la récurrence **[A]** des homographies en considérant les fractions a/b, b/r_2, r_2/r_3, ... [4]

1. on utilise parfois la notation $a \wedge b$, mais comme je n'arrive jamais à me rappeler si c'est $a \wedge b$ ou $a \vee b$, je préfère ici $(a\,,b)$. J'aurais peut-être dû utiliser $\mathrm{pgcd}(a, b)$.
2. Attention donc que je note ici r_2 le reste de la première étape.
3. sauf si $b = 1$...
4. voir aussi http://jf.burnol.free.fr/agreg171122fractionscontinues.pdf.

Car $a/b = q_1 + (b/r_2)^{-1}$, $b/r_2 = q_2 + (r_2/r_3)^{-1}$, ... donc on considère les homographies $\phi_{q_n}(t) = q_n + t^{-1} = (q_n \cdot t + 1)/(1 \cdot t + 0)$ dont les matrices associées sont les

$$Q_n = \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}$$

Ainsi,

$$\frac{r_{n-1}}{r_n} = \phi_{q_n}\left(\frac{r_n}{r_{n+1}}\right)$$

ou plutôt, de manière un peu plus précise

$$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = Q_n \begin{pmatrix} r_n \\ r_{n+1} \end{pmatrix}$$

qui n'est autre qu'une ré-écriture de la relation **[A]**.

Au final les étapes sont rassemblées en un produit matriciel :

[B] $$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} d \\ 0 \end{pmatrix}$$

J'ai noté $d = r_N$ le PGCD de a et de b, comme il est traditionnel.

2 Théorème réciproque

Réciproquement partons d'entiers N, d, $q_1, \ldots q_N$ tous au moins égaux à 1 et formons :

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} d \\ 0 \end{pmatrix}$$

Ceci correspond-t-il à l'algorithme d'Euclide partant de (a, b) ? Pour cela, supposons $0 \leqslant C < B$, $q \geqslant 1$ et formons :

$$\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} B \\ C \end{pmatrix}$$

Donc $A = qB + C$, et C est le reste de la division euclidienne de A par B, ok. Mais peut-on continuer avec un autre q et A, B à la place de B, C ? pour cela il faut regarder si $B < A$. C'est vrai avec une unique exception : **$q = 1$ et $C = 0$**. Notre théorème est donc le suivant :

Théorème 1. *Il y a une correspondance biunivoque entre le déroulement de l'algorithme d'*Euclide *pour les couples* (a, b) *avec* $a > b > 0$ *et les écritures matricielles*

$$\textbf{[C]} \quad \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} d \\ 0 \end{pmatrix}$$

avec $d \geqslant 1$, $N \geqslant 1$, $q_1, \ldots, q_{N-1} \geqslant 1$ *et* $\mathbf{q_N \geqslant 2}$. *Si l'on veut autoriser* $a = b > 0$ *alors il faut dire plutôt : avec* $N \geqslant 1$, $q_1, \ldots, q_N \geqslant 1$, *et* $q_N \geqslant 2$ *si* $N \geqslant 2$.

3 Bézout : descendre ou remonter ?

Écrivons :

$$\textbf{[D]} \quad \begin{pmatrix} \alpha_N & \gamma_N \\ \beta_N & \delta_N \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix} = M$$

De **[C]** il vient :

$$\alpha_N = \frac{a}{d} \quad \beta_N = \frac{b}{d}$$

Le déterminant est multiplicatif, donc

$$\delta_N \alpha_N - \gamma_N \beta_N = (-1)^N$$

On a ainsi une identité de Bézout :

$$\textbf{[E]} \quad \delta_N a - \gamma_N b = (-1)^N d$$

Traditionnellement on obtient une identité de Bézout en « remontant » les calculs. Est-ce la même identité que ci-dessus ?

La méthode de l'École fait

$$\begin{aligned} d = r_N &= r_{N-2} - q_{N-1} r_{N-1} \\ &= r_{N-2} - q_{N-1}(r_{N-3} - q_{N-2} r_{N-2}) \\ &= -q_{N-1} r_{N-3} + (1 + q_{N-1} q_{N-2}) r_{N-2} \\ &= -q_{N-1} r_{N-3} + (1 + q_{N-1} q_{N-2})(r_{N-4} - q_{N-3} r_{N-3}) \\ &= (1 + q_{N-1} q_{N-2}) r_{N-4} - (q_{N-1} + (1 + q_{N-1} q_{N_2}) q_{N-3}) r_{N-3} \\ &= \ldots \\ &= \lambda_k r_{N-k-1} + \mu_k r_{N-k} \\ &= \ldots \end{aligned}$$

$$= \lambda_{N-1} a + \mu_{N-1} b$$

La récurrence (initialisée par $\lambda_0 = 0$, $\mu_0 = 1$) est

$$\lambda_k r_{N-k-1} + \mu_k r_{N-k} = \lambda_k r_{N-k-1} + \mu_k (r_{N-k-2} - q_{N-k-1} r_{N-k-1}) = \mu_k r_{N-k-2} + (\lambda_k - q_{N-k-1}\mu_k) r_{N-k-1}$$

donc

$$\begin{pmatrix} \lambda_{k+1} \\ \mu_{k+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-k-1} \end{pmatrix} \begin{pmatrix} \lambda_k \\ \mu_k \end{pmatrix}$$

soit au total

[F] $$\begin{pmatrix} \lambda_{N-1} \\ \mu_{N-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-1} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Hmm... est-il inquiétant que q_N n'apparaisse pas, et sont-ce vraiment les coefficients fournis par l'équation **[E]** ?

Soyons un peu astucieux :

$$\begin{pmatrix} \lambda_{N-1} \\ \mu_{N-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_N \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (!!)$$
$$= \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Panique à bord, comment relier cela à la matrice M de **[D]** :

$$M = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix},$$

car si on prend l'inverse on va intervertir l'ordre, non ?

Miracle : toutes nos petites matrices sont symétriques, donc

$$^tM = \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}$$
$$\Longrightarrow \ (^tM)^{-1} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix}^{-1}$$

Et nous obtenons finalement

[G] $$\begin{pmatrix} \lambda_{N-1} \\ \mu_{N-1} \end{pmatrix} = (^tM)^{-1} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha_N & \beta_N \\ \gamma_N & \delta_N \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (-1)^N \begin{pmatrix} \delta_N & -\beta_N \\ -\gamma_N & \alpha_N \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (-1)^N \begin{pmatrix} \delta_N \\ -\gamma_N \end{pmatrix}$$

et la relation $\lambda_{N-1} a + \mu_{N-1} b = d$ obtenue par la méthode de l'École est $(-1)^N(\delta_N a - \gamma_N b) = d$ soit en effet **[E]**. Ouf !

L'avantage du produit matriciel

$$M = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix}$$

est de ne comporter que des nombres positifs, on a donc moins de risques de s'embrouiller dans les calculs. Mais multiplier des matrices c'est beaucoup de travail non ? a-t-on vraiment gagné ? On va voir dans la section suivante comment faire.

4 Une récurrence d'ordre deux

Posons

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, M_1 = Q_1, M_2 = Q_1Q_2, \ldots, M_N = M = Q_1 \cdots Q_N$$

Par récurrence on prouve que ces matrices ont la structure suivante :

Théorème 2. *On a* $M_n = (X_n \mid X_{n-1})$ *avec* $X_{-1} = \binom{0}{1}$, $X_0 = \binom{1}{0}$, *et* $X_{n+1} = q_{n+1}X_n + X_{n-1}$.

La matrice $\begin{pmatrix} \gamma_N \\ \delta_N \end{pmatrix}$ est la colonne de droite de $M = M_N$, donc aussi la colonne de gauche de la matrice M_{N-1}. La conclusion est :

Théorème 3. *Définissons par récurrence des suites finies* (v_n), (v'_n), (u_n), (u'_n) *suivant les formules*

$$\begin{aligned} v'_0 &= 0, \quad u'_0 = 1 \\ v_0 &= 1, \quad u_0 = 0 \\ v'_{n+1} &= v_n, \quad u'_{n+1} = u_n \\ v_{n+1} &= q_{n+1}v_n + v'_n \\ u_{n+1} &= q_{n+1}u_n + u'_n \end{aligned}$$

alors si $a, b > 0$ *et* $q_1, \ldots, q_N$ *sont les quotients successifs dans l'algorithme d'*Euclide *qui calcule le PGCD* d, *on a* $v_N = a/d$, $u_N = b/d$ *et* v_{N-1} *et* u_{N-1} *(dont le calcul ne nécessite pas* q_N*) fournissent une identité de* Bézout

$$u_{N-1}a - v_{N-1}b = (-1)^N d \, .$$

Remarque : il serait plus logique d'intervertir les lettres u et v car a est « au-dessus de » b mais u est « en-dessous de » v, mais bon bref, la notation $ua \pm vb$ est traditionnelle avec Bézout.

Cet algorithme est lié à celui que les informaticiens appellent « algorithme d'Euclide étendu » mais en général leurs formules de récurrences ont un signe moins et fournissent un couple U_N, V_N avec $U_Na + V_Nb = d$. Mais ils calculent en fait la même identité de Bézout que nous. Enfin j'espère… faudrait que je vérifie.

5 Application du théorème réciproque : construire un exercice

Exemple : $N = 4$, $q_1 = 7$, $q_2 = 4$, $q_3 = 2$, $q_4 = 5$. Je calcule à partir de la droite le produit matriciel par des combinaisons de lignes :

$$\begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix} \to \begin{pmatrix} 11 & 2 \\ 5 & 1 \end{pmatrix} \to \begin{pmatrix} 49 & 9 \\ 11 & 2 \end{pmatrix} \to \begin{pmatrix} 354 & 65 \\ 49 & 9 \end{pmatrix}$$

Cela nous donne une matrice de déterminant 1. Et vous savez d'après notre Théorème 1 qu'en donnant à vos élèves : *calculer le* PGCD *de* 2478 *(*7×354*) et de* 343 *(*7×49*)*, ils trouveront 7 après 4 étapes, et les quotients successifs seront $q_1 = 7$, $q_2 = 4$, $q_3 = 2$, $q_4 = 5$. De plus vous connaissez à l'avance l'identité de Bézout

$$9 \times 2478 - 65 \times 343 = 7$$

qu'ils pourront (peut-être) retrouver en « remontant » les calculs ! Il faut absolument encourager les calculs, et donc l'exercice terminera en apothéose lorsqu'ils vérifieront à la main que cette identité fonctionne.

6 Nombre d'étapes et nombres de Fibonacci

Note : *la v1 de 2011 comportait une erreur (décalage de* 1 *dans l'indice des nombres de* Fibonacci *pour les minorations de* γ_N *et* δ_N*). Heureusement les minorations de* α_N *et* β_N *étaient correctes donc le Théorème qui suit également.*

On suppose $a > b > 0$.

Comme $q_1 \geqslant 1, \ldots, q_N \geqslant 2$, il est vrai et aussi facile de montrer par récurrence :

$$\begin{pmatrix} \alpha_N & \gamma_N \\ \beta_N & \delta_N \end{pmatrix} = \overbrace{\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_{N-1} & 1 \\ 1 & 0 \end{pmatrix}}^{N-1 \text{ termes}} \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix} \geqslant \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{N-1} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

au sens où tous les coefficients de la matrice de gauche sont au moins égaux à ceux de la matrice de droite.

Les nombres de Fibonacci, $F_{-1} = 1$, $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_{n+2} = F_n + F_{n+1}$ permettent d'exprimer la matrice minorante :

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{N-1} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} F_N & F_{N-1} \\ F_{N-1} & F_{N-2} \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2F_N + F_{N-1} & F_N \\ 2F_{N-1} + F_{N-2} & F_{N-1} \end{pmatrix} = \begin{pmatrix} F_{N+2} & F_N \\ F_{N+1} & F_{N-1} \end{pmatrix}$$

Ainsi :

[H] $\gamma_N \geqslant F_N, \quad \delta_N \geqslant F_{N-1},$

[I] $\alpha_N \geqslant F_{N+2}, \quad \beta_N \geqslant F_{N+1}$

Mais nous savons que :

$$\alpha_N = \frac{a}{d} \leqslant a, \qquad \beta_N = \frac{b}{d} \leqslant b$$

Cela nous donne le Théorème suivant :

Théorème 4. *Le nombre* N *d'étapes qui sont nécessaires pour calculer le* PGCD *de* a *et de* b *(*$0 < b < a$*) par l'algorithme d'*Euclide *est majoré par les inégalités* $F_{N+1} \leqslant b$ *et* $F_{N+2} \leqslant a$*. Ainsi pour estimer* N *on calcule* k *tel que* $F_k \leqslant b < F_{k+1}$*. Alors* $N \leqslant k - 1$*. Mais si* a *est lui aussi* $< F_{k+1}$ *alors en fait* $N \leqslant k - 2$*.*

Comme on a la formule explicite :

$$F_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}, \qquad \alpha = \Phi = \frac{1 + \sqrt{5}}{2}, \quad \beta = -\alpha^{-1} = \frac{1 - \sqrt{5}}{2} = 1 - \Phi, \quad -1 < \beta < 0\ ,$$

on voit que k est contraint par

$$\ln(\alpha^k - \beta^k) \leqslant \ln(b) + \ln(\alpha - \beta)$$

$$k \ln(\alpha) \leqslant \ln(b) + \ln(\alpha - \beta) - \ln\left(1 - (\beta/\alpha)^k\right)$$

Bien sûr j'ai supposé k au moins égal à 1 pour éviter d'avoir ln(0), et comme $b \geqslant 1 = F_2$, en fait on peut même supposer $k \geqslant 2$ dans ce qui suit qui recherche le plus grand k possible.

Comme β/α est négatif (et de valeur absolue inférieure à 1), la valeur maximale de

$$-\ln(1 - (\beta/\alpha)^k)$$

est obtenue pour k pair le plus petit possible, donc $k = 2$. Donc :

$$k \ln(\alpha) \leqslant \ln(b) + \ln(\alpha - \beta) - \ln(1 - (\beta/\alpha)^2) = \ln(b) + \ln\left(\alpha^2 \frac{1}{\alpha + \beta}\right) = \ln(b) + 2\ln(\alpha)$$

Comme notre estimation du nombre N d'étapes est $N \leqslant k - 1$ nous obtenons :

Théorème 5. *Le nombre* N *d'étapes est majoré par* $\dfrac{\ln b}{\ln \Phi} + 1$ *et aussi par* $\dfrac{\ln a}{\ln \Phi}$ *avec* Φ *le nombre d'or.*

La deuxième estimation est meilleure que la première s'il existe un entier x avec $\frac{\ln a}{\ln \Phi} < x \leqslant \frac{\ln b}{\ln \Phi} + 1$. On aurait à la fois

$$a < \Phi^x \qquad \text{et} \qquad \Phi^{x-1} \leqslant b$$

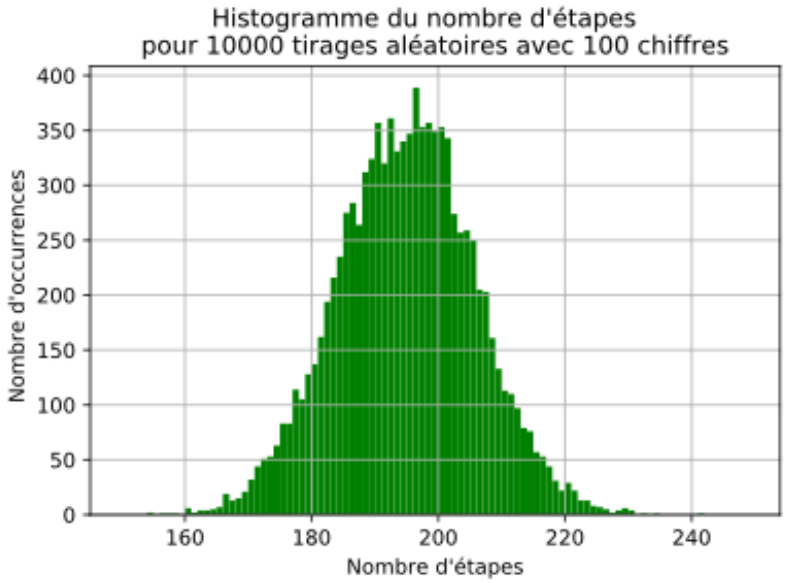
Ainsi s'il existe un entier x avec $\Phi^{x-1} \leqslant b < a < \Phi^x$ l'estimation du nombre d'étapes qui utilise b donne $N \leqslant x$ mais celle qui utilise a donne $N \leqslant x-1$ soit 1 étape en moins. Donc utiliser la formule avec a ne peut nous faire gagner que 1 et en général nous fait plutôt perdre, puisque a n'est pas limité supérieurement. De toute façon le véritable nombre d'étapes peut être bien inférieur encore.

Comme en fait F_k est proche de $\sqrt{\frac{1}{5}}\Phi^k$, la méthode plus exacte avec les nombres de Fibonacci donnerait quelque chose approximativement comme $N \lesssim \frac{\ln b}{\ln \Phi} + \frac{\ln 5^{1/2}}{\ln \Phi} - 1 = \frac{\ln b}{\ln \Phi} + 0{,}672\,275\,9\ldots$, donc au mieux on pourrait gagner 1 dans l'estimation de N.

On connaît de manière assez précise le comportement du nombre d'étapes N :

Théorème 6 (Hensley 1994, après Heilbronn, Dixon, Porter, Knuth, Norton,...)**.** *Lorsque* $X \to \infty$*, le nombre d'étapes dans l'algorithme d'*Euclide *pour les couples* $1 \leqslant b \leqslant a \leqslant X$ *a une distribution qui est asymptotiquement proche d'une loi normale d'espérance* $12\pi^{-2} \log 2 \log X$ *et de variance* $C_1 \log X$ *avec* C_1 *une autre constante.*

Voici un histogramme obtenu en prenant 10000 fois des nombres entiers aléatoires de 100 chiffres décimaux.



Le « coût moyen de l'algorithme d'Euclide » par chiffre décimal est $12\frac{\log 2 \log 10}{\pi^2} = 1{,}940\,540\ldots$. On note que la majoration du Théorème 5 est aussi linéaire en le nombre de chiffres décimaux : $\log 10 / \log \Phi = 4{,}784\,971\ldots$, ce qui est un peu moins que 2,5 fois la valeur moyenne $1{,}940\,540\ldots$.