La « probabilité » que r entiers soient premiers entre-eux

Marc Lorenzi

27 avril 2024

1 Introduction

1.1 Densité

Pour tout entier $n \geq 1$, on note $\mathbb{N}_n = [\![1, n]\!]$.

Soit $r \in \mathbb{N}^*$. Pour tout $n \geq 1$ et toute partie E de $(\mathbb{N}^*)^r$, notons

$$E_n = E \cap (\mathbb{N}_n)^r$$

Définition 1. Une partie E de $(\mathbb{N}^*)^r$ possède une densité si $|E_n|/n^r$ a une limite lorsque n tend vers l'infini. La *densité* de E est alors

$$\mathbb{D}(E) = \lim_{n\to\infty} \frac{|E_n|}{n^r}$$

Intuitivement, la densité de E est la « proportion » d'éléments de $(\mathbb{N}^*)^r$ qui appartiennent à E. Dans la suite de l'article, r désigne un entier supérieur ou égal à 2.

1.2 Une partie de $(\mathbb{N}^*)^r$

Nous allons nous intéresser à l'ensemble des r-uplets d'entiers qui sont premiers entre-eux, c'est à dire à l'ensemble

$$G^r = \{(u_1, \ldots, u_r) \in (\mathbb{N}^*)^r : \text{pgcd}(u_1, \ldots, u_r) = 1\}$$

L'objet de l'article est de montrer que G^r possède une densité et de calculer cette densité. Voici G^2_{53}. Les éléments de G^2_{53} sont les pixels noirs.

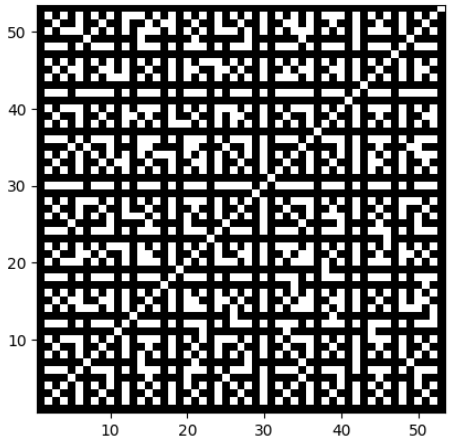

FIGURE 1 – L'ensemble G_{53}^2

La figure ci-dessous montre $|G_n^2|/n^2$ pour $n \in [\![1000, 5000]\!]$. On constate un comportement assez compliqué de cette quantité, mais lorsque n augmente, les valeurs possibles de celle-ci semblent se resserrer, ce qui est un signe d'une possible convergence.

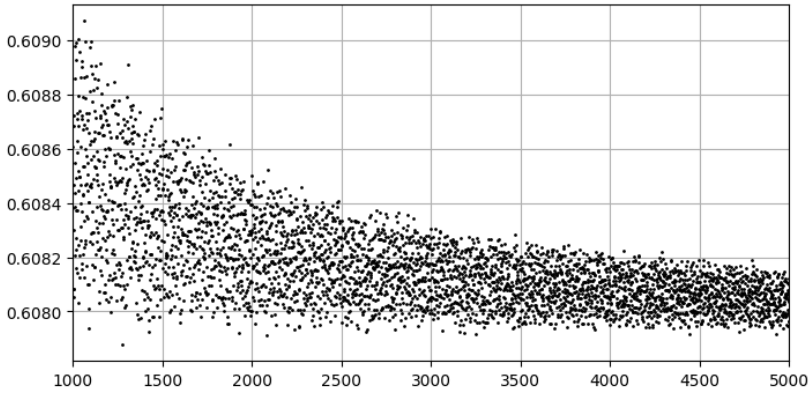

FIGURE 2 – $|G_n^2|/n^2$

1.3 Première approche

Quelle est la densité ℓ de G^r ? Un argument heuristique est le suivant. Tout r-uplet $(a_1, \ldots, a_r) \in (\mathbb{N}^*)^r$ s'écrit de façon unique $a_1 = \delta u_1, \ldots, a_r = \delta u_r$ où $\delta = \text{pgcd}(a_1, \ldots, a_r)$ et $(u_1, \ldots, u_r) \in G^r$. On a donc

$$(\mathbb{N}^*)^r = \bigcup_{\delta=1}^{\infty} \delta G^r$$

et la réunion est disjointe. Quelle est la densité de δG^r ? Pour tout $n \geq 1$,

$$(\delta G^r)_n = (\delta G^r) \cap \mathbb{N}_n^r = \delta G_{\lfloor n/\delta \rfloor}^r$$

et donc

$$|(\delta G^r)_n| = |G^r_{\lfloor n/\delta \rfloor}|$$

On en déduit

$$\frac{1}{n^r}|(\delta G^r)_n| = \frac{1}{\delta^r}\frac{|G^r_{\lfloor n/\delta \rfloor}|}{(n/\delta)^r} \underset{n\to\infty}{\longrightarrow} \frac{\ell}{\delta^r}$$

Ainsi,

$$\mathbb{D}(\delta G^r) = \frac{\ell}{\delta^r}$$

De là,

$$1 = \mathbb{D}((\mathbb{N}^*)^r) = \sum_{\delta=1}^{\infty} \mathbb{D}(\delta G^r) = \sum_{\delta=1}^{\infty} \frac{\ell}{\delta^r}$$

d'où

$$\ell \sum_{\delta=1}^{\infty} \frac{1}{\delta^r} = \ell\zeta(r) = 1$$

et donc $\ell = 1/\zeta(r)$ où ζ est la *fonction de Riemann*. Ce « raisonnement » comporte deux failles.

- Nous ne savons pas si $\mathbb{D}(G^r)$ existe, ce qui est évidemment une énorme faille.
- Contrairement à une probabilité, la fonction de densité $\mathbb{D}$ n'est pas dénombrablement additive. Par exemple, $(\mathbb{N}^*)^r$ est une réunion dénombrable disjointe de singletons qui sont de densité nulle, alors que la densité de $(\mathbb{N}^*)^r$ est égale à 1.

Nous allons effectivement montrer que $\mathbb{D}(G^r)$ existe et vaut $1/\zeta(r)$ mais pour cela il va nous falloir travailler un peu.

2 La fonction de Möbius

2.1 La fonction μ

Définition 2. La *fonction de Möbius* est la fonction $\mu : \mathbb{N}^* \longrightarrow \{-1, 0, 1\}$ définie pour tout $n \in \mathbb{N}^*$ par

- $\mu(n) = 0$ si n possède un facteur carré.
- $\mu(n) = (-1)^k$ si n est le produit de k nombres premiers distincts, où $k \in \mathbb{N}$.

En particulier, $\mu(1) = 1$ car 1 est le produit de zéro nombre premier distinct. La fonction de Möbius vérifie de nombreuses propriétés et joue un rôle important en théorie des nombres. Les premières valeurs de la fonction μ sont données dans le tableau ci-dessous.

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$\mu(n)$	1	-1	-1	0	-1	1	-1	-1	1	1	-1	0	-1

Voici le graphe de μ sur l'intervalle $[\![1, 100]\!]$.

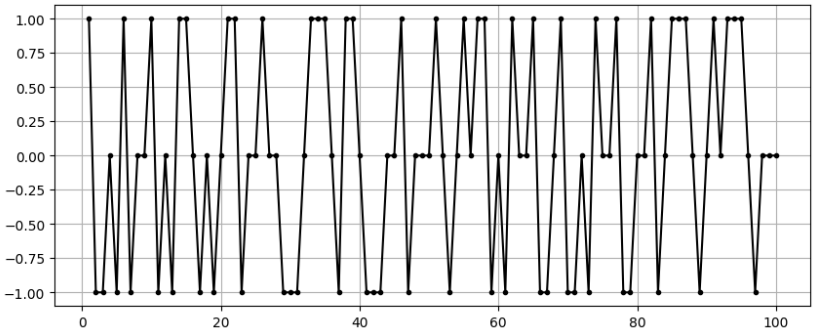

FIGURE 3 – La fonction de Möbius

2.2 Une propriété importante

Proposition 1. *Pour tout entier $n \geq 2$,*

$$\sum_{d|n} \mu(d) = 0$$

Démonstration. Soit $n \geq 2$. Posons

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

où $k \geq 1$, les p_i sont des nombres premiers distincts et les α_i des entiers non nuls. Les diviseurs de n sont les entiers

$$d = p_1^{\beta_1} \dots p_k^{\beta_k}$$

où, pour tout $i \in [\![1, k]\!]$, $\beta_i \in [\![0, \alpha_i]\!]$. Pour un tel diviseur d, si l'un des β_i est différent de 0 ou 1, $\mu(d) = 0$. Pour tout $j \in [\![0, k]\!]$ il y a $\binom{k}{j}$ diviseurs d de n qui sont le produit de j nombres premiers choisis parmi $p_1, \dots, p_k$. Pour ces diviseurs, on a $\mu(d) = (-1)^j$. Ainsi,

$$\sum_{d|n} \mu(d) = \sum_{j=0}^{k} (-1)^j \binom{k}{j} = (1-1)^k = 0$$

□

2.3 Une série reliée à μ

Une série va jouer un rôle central dans la suite de l'article. Il s'agit de la série

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k^r}$$

Cette série est absolument convergente. En effet, pour tout $k \in \mathbb{N}^*$,

$$\left|\frac{\mu(k)}{k^r}\right| \leq \frac{1}{k^r}$$

Comme $r \geq 2$, $1/k^r$ est le terme général d'une série de Riemann convergente. Nous allons déterminer la somme de cette série. Pour cela, commençons par un lemme qui est un cas particulier d'un résultat plus général sur les *séries de Dirichlet*.

Lemme 2. *Soient $\sum_{n\geq 1} \frac{a_n}{n^r}$ et $\sum_{n\geq 1} \frac{b_n}{n^r}$ deux séries absolument convergentes à termes réels ou complexes. On a alors*

$$\sum_{n\geq 1} \frac{a_n}{n^r} \sum_{n\geq 1} \frac{b_n}{n^r} = \sum_{n\geq 1} \frac{c_n}{n^r}$$

où

$$c_n = \sum_{d|n} a_d b_{n/d}$$

Démonstration. Les deux séries $\sum_{n\geq 1} \frac{a_n}{n^r}$ et $\sum_{n\geq 1} \frac{b_n}{n^r}$ sont absolument convergentes. Par le théorème de Fubini, la famille $(a_n b_m/(mn)^r)_{(n,m)\in\mathbb{N}^*\times\mathbb{N}^*}$ est sommable et

$$A = \sum_{n=1}^{\infty} \frac{a_n}{n^r} \sum_{m=1}^{\infty} \frac{b_m}{m^r} = \sum_{(n,m)\in\mathbb{N}^*\times\mathbb{N}^*} \frac{a_n b_m}{(mn)^r}$$

Posons $k = mn$ dans l'expression ci-dessus. Le théorème de sommation par paquets permet de regrouper les termes à k constant pour obtenir

$$\begin{aligned} A &= \sum_{k=1}^{\infty} \left(\frac{1}{k^r} \sum_{mn=k} a_n b_m \right) \\ &= \sum_{k=1}^{\infty} \left(\frac{1}{k^r} \sum_{n|k} a_n b_{k/n} \right) \\ &= \sum_{k=1}^{\infty} \frac{c_k}{k^r} \end{aligned}$$

□

Proposition 3.

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} = \frac{1}{\zeta(r)}$$

Démonstration. Considérons les deux séries $\sum_{k=1}^{\infty} \frac{\mu(k)}{k^r}$ et $\sum_{m=1}^{\infty} \frac{1}{m^r}$. Ces

deux séries sont absolument convergentes. Par le lemme 2,

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k^r} \sum_{m=1}^{\infty} \frac{1}{m^r} = \sum_{n=1}^{\infty} \frac{c_n}{n^r}$$

où

$$c_n = \sum_{d|n} \mu(d)$$

Par la proposition 1, si $n \geq 2$ alors $c_n = 0$. Ainsi,

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} \sum_{m=1}^{\infty} \frac{1}{m^2} = c_1 = 1$$

□

3 La densité de G^r

3.1 Formule du crible

Proposition 4. *Pour tout $n \geq 1$,*

$$|G_n^r| = \sum_{k=1}^{\infty} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^r$$

La somme ci-dessus est en réalité une somme finie, puisque la partie entière est nulle dès que $k > n$.

Démonstration. Notons $\mathcal{P}$ l'ensemble des entiers premiers positifs. Soit $n \geq 1$. Pour tout $p \in \mathcal{P}$, soit

$$S_p = \{(u_1, \ldots, u_r) \in \mathbb{N}_n^r : p \mid u_1, \ldots, p \mid u_r\}$$

Des entiers sont premiers entre-eux si et seulement si ils n'ont aucun facteur *premier* commun. On a donc

$$|G_n^r| = |\mathbb{N}_n^r \setminus \bigcup_{p \in \mathcal{P}} S_p|$$

La réunion ci-dessus est en réalité une union finie. En effet, pour tout $p > n$, $S_p = \emptyset$. Par la formule du crible,

$$|G_n^r| = |\mathbb{N}_n^r| - \sum_{j=1}^{\infty} (-1)^{j-1} \sum_{p_1 < \ldots < p_j} |S_{p_1} \cap \ldots \cap S_{p_j}|$$

La somme sur j et les sommes sur $p_1, \ldots, p_j$ sont en fait des sommes finies. Pour tout $j \geq 1$, soient $p_1, \ldots, p_j$ des nombres premiers distincts. Soit $(u_1, \ldots, u_r) \in \mathbb{N}_n^r$. On a $(u_1, \ldots, u_r) \in S_{p_1} \cap \ldots \cap S_{p_j}$ si et seulement si chacun des p_i divise

$u_1, \ldots, u_r$, c'est à dire si et seulement si le produit des p_i divise $u_1, \ldots, u_r$. On a donc

$$|S_{p_1} \cap \ldots \cap S_{p_j}| = \left\lfloor \frac{n}{p_1 \ldots p_j} \right\rfloor^r$$

Ainsi,

$$|G_n^r| = n^r + \sum_{j=1}^{\infty} (-1)^j \sum_{p_1 < \ldots < p_j} \left\lfloor \frac{n}{p_1 \ldots p_j} \right\rfloor^r$$

Comparons avec la somme donnée par la proposition. Soit $k \geq 1$. Si $k = 1$ alors $\mu(k) \lfloor n/k \rfloor^r = n^r$. Si $k \geq 2$ a un facteur carré alors $\mu(k) \lfloor n/k \rfloor^r = 0$. Enfin, si $k = p_1 \ldots p_j$ est le produit de j nombres premiers distincts, alors $\mu(k) \lfloor n/k \rfloor^r = (-1)^j \lfloor n/(p_1 \ldots p_j) \rfloor^r$. □

3.2 Densité, enfin

Proposition 5. *Lorsque n tend vers l'infini,*

$$\frac{|G_n^r|}{n^r} \longrightarrow \sum_{k=1}^{\infty} \frac{\mu(k)}{k^r}$$

Démonstration.

$$\begin{aligned}
|G_n^r| - \sum_{k=1}^{\infty} \mu(k) \left(\frac{n}{k}\right)^r &= \sum_{k=1}^{\infty} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^r - \sum_{k=1}^{\infty} \mu(k) \left(\frac{n}{k}\right)^r \\
&= \sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^r - \sum_{k=1}^{\infty} \mu(k) \left(\frac{n}{k}\right)^r \\
&= \sum_{k=1}^{n} \mu(k) \left(\left\lfloor \frac{n}{k} \right\rfloor^r - \left(\frac{n}{k}\right)^r \right) - \sum_{k=n+1}^{\infty} \mu(k) \left(\frac{n}{k}\right)^r \\
&= S_1 - S_2
\end{aligned}$$

Pour tout $x \in \mathbb{R}_+$,

$$|x^r - \lfloor x \rfloor^r| = (x - \lfloor x \rfloor) \sum_{k=0}^{r-1} x^k \lfloor x \rfloor^{r-1-k}$$

On a $x - \lfloor x \rfloor \leq 1$ et pour tout $k \in [\![0, r-1]\!]$,

$$x^k \lfloor x \rfloor^{r-1-k} \leq (x+1)^{r-1}$$

De là,

$$|x^r - \lfloor x \rfloor^r| \leq r(x+1)^{r-1}$$

On a donc

$$\begin{aligned}
|S_1| &= \left|\sum_{k=1}^{n} \mu(k)\left(\left\lfloor\frac{n}{k}\right\rfloor^r - \left(\frac{n}{k}\right)^r\right)\right| \\
&\leq \sum_{k=1}^{n}\left|\left\lfloor\frac{n}{k}\right\rfloor^r - \left(\frac{n}{k}\right)^r\right| \\
&\leq r\sum_{k=1}^{n}\left(\frac{n}{k}+1\right)^{r-1} \\
&\leq r\sum_{k=1}^{n}\left(\frac{2n}{k}\right)^{r-1} \\
&= r2^{r-1}n^{r-1}\sum_{k=1}^{n}\frac{1}{k^{r-1}}
\end{aligned}$$

Ici, il s'agit de distinguer selon que $r = 2$ ou pas. Si $r \geq 3$,

$$\sum_{k=1}^{n}\frac{1}{k^{r-1}} \leq \zeta(r-1)$$

et

$$\frac{1}{n^r}r2^{r-1}n^{r-1}\zeta(r-1) = \frac{1}{n}r2^{r-1}\zeta(r-1) = O\left(\frac{1}{n}\right) \underset{n\to\infty}{\longrightarrow} 0$$

Ainsi, S_1/n^r tend vers 0 lorsque n tend vers l'infini. Dans le cas où $r = 2$,

$$\sum_{k=1}^{n}\frac{1}{k^{r-1}} = \sum_{k=1}^{n}\frac{1}{k} = H_n$$

où H_n est le $k$ième *nombre harmonique*. On a

$$\frac{1}{n^r}r2^{r-1}n^{r-1}H_n = \frac{1}{n}2H_n = O\left(\frac{\ln n}{n}\right) \underset{n\to\infty}{\longrightarrow} 0$$

Ainsi, S_1/n^2 tend aussi vers 0 lorsque n tend vers l'infini. Passons à la deuxième somme.

$$|S_2| = \left|\sum_{k=n+1}^{\infty}\mu(k)\left(\frac{n}{k}\right)^r\right| \leq n^r\sum_{k=n+1}^{\infty}\frac{1}{k^r} = n^rO\left(\frac{1}{n^{r-1}}\right) = O(n)$$

De là,

$$\frac{S_2}{n^r} = \frac{1}{n^r}O(n) = O\left(\frac{1}{n^{r-1}}\right)$$

et donc S_2/n^r tend vers 0 lorsque n tend vers l'infini. □

Remarquons que nous avons aussi obtenu la vitesse de convergence de $\frac{|G_n^r|}{n^r}$ vers sa limite.

- Si $n = 2$,

$$\frac{|G_n^2|}{n^2} = \sum_{k=1}^{\infty}\frac{\mu(k)}{k^2} + O\left(\frac{\ln n}{n}\right)$$

  La convergence est dans ce cas relativement lente. Nous avons déjà remarqué ce phénomène au début de l'article.

- Si $n \geq 3$,

$$\frac{|G_n^r|}{n^r} = \sum_{k=1}^{\infty} \frac{\mu(k)}{k^r} + O\left(\frac{1}{n}\right)$$

La convergence est cette fois-ci (un peu) plus rapide.

En réunissant les propositions 3 et 5 nous obtenons la

Proposition 6. *L'ensemble G^r possède une densité qui est*

$$\mathbb{D}(G^r) = \frac{1}{\zeta(r)}$$

3.3 Compléments

Voici $\mathbb{D}(G^r)$ pour les premières valeurs de r.

r	$\mathbb{D}(G^r)$
2	0.607890
3	0.831907
4	0.923938
5	0.964387
6	0.982953
7	0.991720
8	0.995939
9	0.997996
10	0.999006

Et voici la courbe de $x \longmapsto 1 - 1/\zeta(x)$ pour $x \in [1, 20]$. Lorsque x tend vers l'infini, $1/\zeta(x)$ tend vers 1. Informellement, pour le problème qui nous intéresse, plus r est « grand », plus la « probabilité » que r entiers soient premiers entre eux est « grande » et cette probabilité tend vers 1 lorsque r tend vers l'infini.

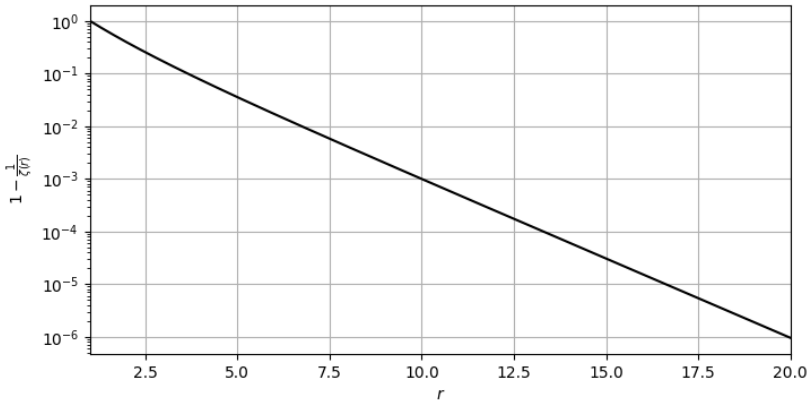

FIGURE 4 – L'inverse de ζ

4 Un autre problème

Quelle est la « probabilité » que r entiers soient premiers entre eux *deux à deux* ? Plus formellement, pour tout $r \geq 1$ soit

$$F^r = \{(u_1, \ldots, u_r) \in (\mathbb{N}^*)^r : \forall i \neq j, \text{pgcd}(u_i, u_j) = 1\}$$

La question est de savoir si F^r possède une densité. En cas de réponse positive, quelle est cette densité ? Cette question est plus délicate que celle dont nous nous sommes occupés et nécessite un article à elle seule. Nous nous contenterons de la réponse. Rappelons que $\mathcal{P}$ est l'ensemble des nombres premiers.

Proposition 7. *L'ensemble F^r possède une densité qui est*

$$\mathbb{D}(F^r) = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right)^{r-1} \left(1 + \frac{r-1}{p}\right)$$

Voici les premières valeurs de $\mathbb{D}(F^r)$.

r	$\mathbb{D}(F^r)$
2	6.0793×10^{-1}
3	2.8675×10^{-1}
4	1.1488×10^{-1}
5	4.0930×10^{-2}
6	1.3325×10^{-2}
7	4.0346×10^{-3}
8	1.1504×10^{-3}
9	3.1171×10^{-4}
10	8.0813×10^{-5}

Et voici $\mathbb{D}(F^r)$ pour $r \in [\![1, 100]\!]$. Contrairement au problème qui nous a occupés tout au long de cet article, lorsque r tend vers l'infini, $\mathbb{D}(F^r)$ tend vers 0. Plus r est « grand », plus la « probabilité » que r entiers soient premiers entre eux deux à deux est « petite » et cette probabilité tend vers 0 lorsque r tend vers l'infini. Par exemple,

$$\mathbb{D}(F^{100}) < 10^{-76}$$

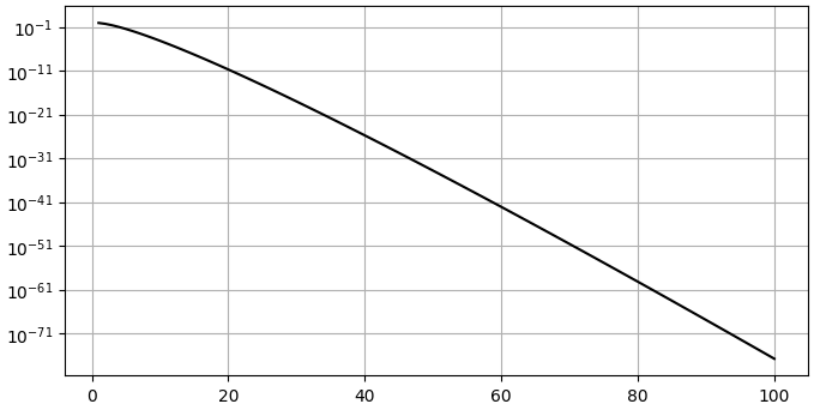

FIGURE 5 – $\mathbb{D}(F^r)$

Bibliographie.

- Gérald Tenenbaum, Introduction to Analytic and Probabilistic Number Theory, Graduate Studies in Mathematics (1995)
- Jörn Steuding, Probabilistic Number Theory (2002). http://www.alternatievewiskunde.nl/QED/prob.pdf
- Marcel K. Goh, On the probability that two integers are relatively prime (2019). https://marcelgoh.ca/misc/proofs/coprime-probability.pdf
- Lászlò Tóth, The probability that k positive integers are pairwise relatively prime (2000).