imagesdesmathématiques
Les mathématiques en mots et en images

Le théorème de Don Quichotte

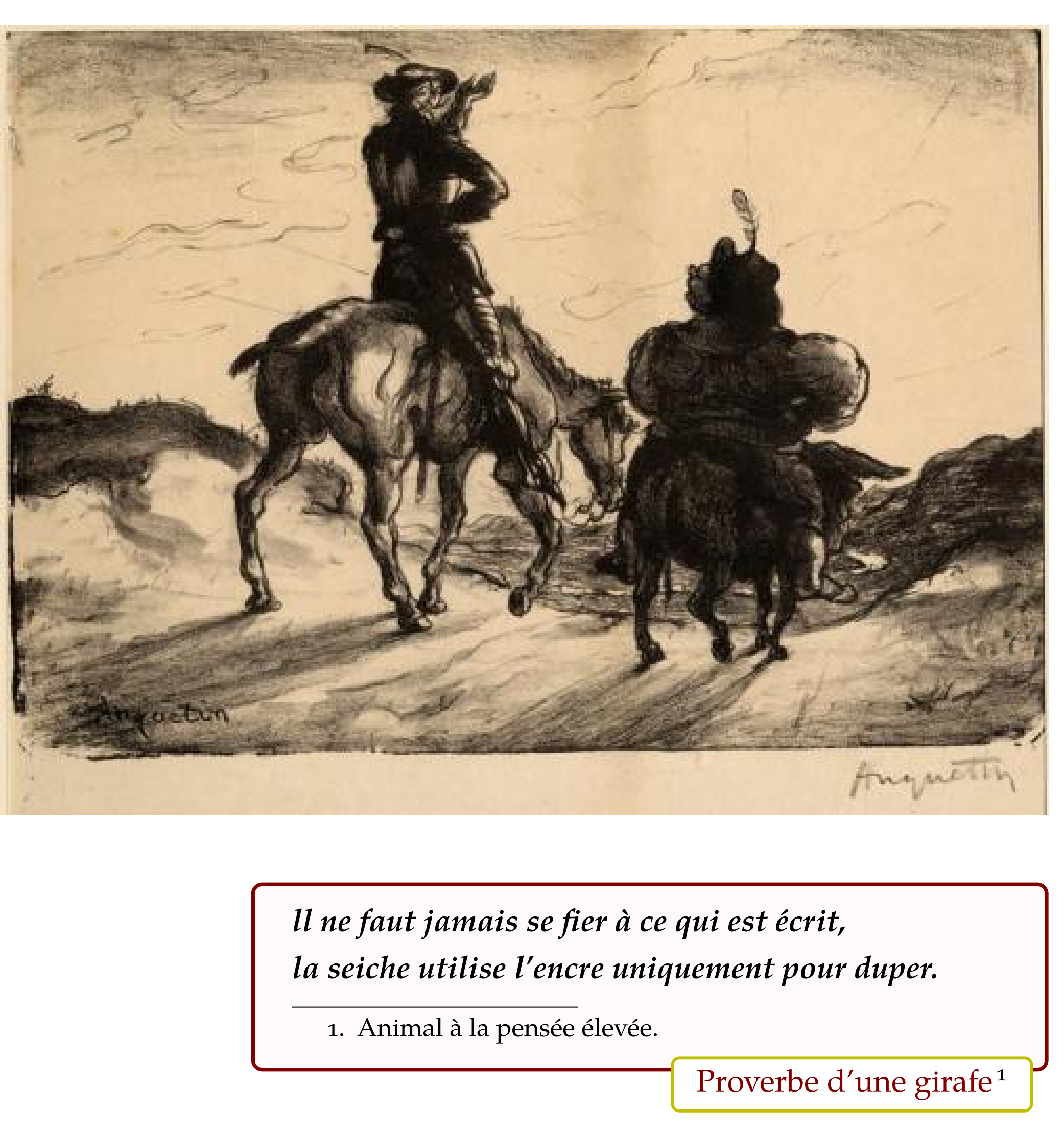
Écrit par **Roland Bacher**

Publié le 22 juillet 2023

DOI : `10.60868/cb15-d975` —

🖌 🖌 🖌 — 15 min ⩽ 🕒 ⩽ 30 min

NOMBRES PREMIERS



> ***Il ne faut jamais se fier à ce qui est écrit,***
> ***la seiche utilise l'encre uniquement pour duper.***
>
> [1] Animal à la pensée élevée.
>
> Proverbe d'une girafe[1]

Cet article a été écrit avec une plume chatouilleuse. Le lecteur allergique peut sauter le prologue et commencer la lecture par le théorème de Don Quichotte.

Don Quichotte veut offrir à sa dame, la sublime Dulcinée du Toboso, du chocolat pour la Saint-Valentin[1]. Selon les canons de l'amour courtois, le parfait galant se procure deux morceaux rectangulaires de taille $a \times b$ et $c \times d$ de ce péché capital. Le nombre total $a \cdot b + c \cdot d$ de carrés doit être un nombre premier car rien ne peut diviser deux amoureux. L'orientation compte. Les deux emballages illustrent le courage du chevalier et la beauté de sa dame : deux morceaux de taille respectivement $a \times b$ et $b \times a$ seront donc considérés comme différents si a et b ne sont pas égaux. Les coutumes barbares du Moyen Âge prescrivent au gentilhomme d'offrir un délicieux morceau de taille $c \times d$ à sa dame et d'endurer stoïquement les inconvénients gastriques liés à la difficile digestion du gros morceau de taille $a \times b$ avec a et b tous les deux strictement supérieurs à c et d. Certains historiens justifient cette tradition par l'homéopathie : la finesse d'un chocolat est inversement proportionnelle à sa quantité. D'autres historiens, plus romantiques, prétendent au contraire que la modestie du chevalier lui impose de ne pas exagérer ses exploits, dépeints sur l'emballage du morceau destiné à son adorée, par une représentation surdimensionnée. J'omets ici une troisième explication, colportée par des mauvaises langues envieuses.

C'est sans aucun doute à cette occasion que Don Quichotte a découvert le résultat suivant qui porte désormais son illustre nom[2] :

Théorème 1 (Don Quichotte)

Tout nombre premier impair p possède exactement $(p+1)/2$ écritures de la forme $p = a \cdot b + c \cdot d$ en tenant compte de l'ordre des facteurs avec a, b, c, d dans $\mathbf{N}$ et $\min(a,b) > \max(c,d)$.

Illustrons ce théorème avec le cas du nombre premier 23. Les $(23+1)/2 = 12$ écritures possibles sont :

$$\begin{array}{cccc} 23 \cdot 1 + 0 \cdot 0 & 1 \cdot 23 + 0 \cdot 0 & 11 \cdot 2 + 1 \cdot 1 & 2 \cdot 11 + 1 \cdot 1 \\ 7 \cdot 3 + 2 \cdot 1 & 3 \cdot 7 + 2 \cdot 1 & 7 \cdot 3 + 1 \cdot 2 & 3 \cdot 7 + 1 \cdot 2 \\ 5 \cdot 4 + 3 \cdot 1 & 4 \cdot 5 + 3 \cdot 1 & 5 \cdot 4 + 1 \cdot 3 & 4 \cdot 5 + 1 \cdot 3 \end{array}$$

Par contre, les expressions $22 \cdot 1 + 1 \cdot 1$, $1 \cdot 19 + 2 \cdot 2$, $3 \cdot 6 + 5 \cdot 1$ et $3 \cdot 1 + 5 \cdot 4$ sont interdites car ces expressions (qui sont pourtant bien de la forme $a \cdot b + c \cdot d$) ne satisfont pas l'inégalité stricte $\min(a,b) > \max(c,d)$.

L'idée de la preuve du théorème de Don Quichotte est de combattre des moulins à vent[3]. L'article [2] en est une transcription en langage moderne. Le lien avec les moulins à vent s'obtient en associant à une solution $p = a \cdot b + c \cdot d$ le sous-réseau $\mathbf{Z}(a,c) + \mathbf{Z}(-d,b)$ d'indice p dans $\mathbf{Z}^2$. Les deux générateurs (a,c) et $(-d,b)$ appartiennent alors respectivement aux voiles noires orientés E-NE et N-NW (utilisant les conventions anglaises pour une rose des vents) de la figure 1 évoquant un moulin à vent.

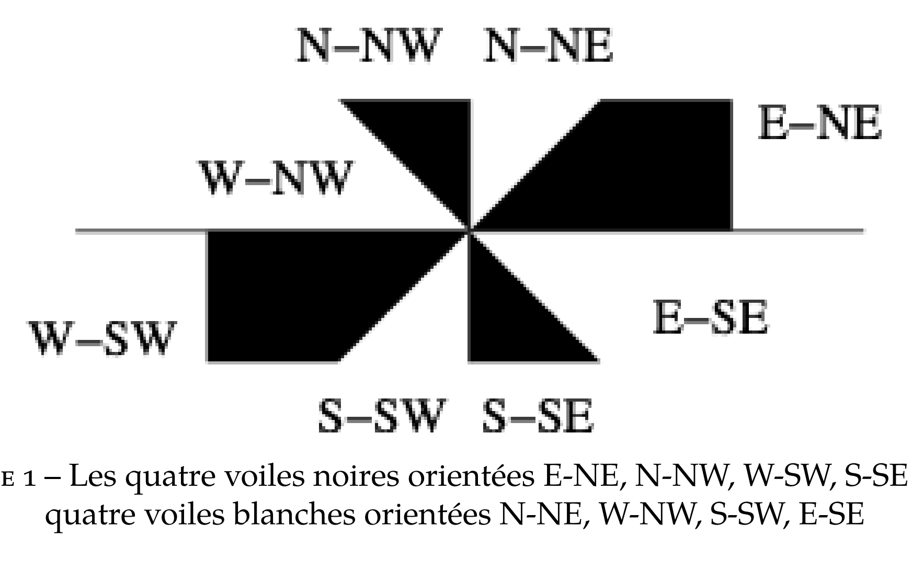


FIGURE 1 – Les quatre voiles noires orientées E-NE, N-NW, W-SW, S-SE et les quatre voiles blanches orientées N-NE, W-NW, S-SW, E-SE

Le théorème de Don Quichotte donne une nouvelle preuve du résultat suivant.

Corollaire 2 (Théorème de Fermat)

Tout nombre premier de la forme $1 + 4n$ est une somme de deux carrés.

Une généralisation de ce résultat décrivant l'ensemble de tous les entiers qui sont sommes de deux carrés était énoncée pour la première fois sous forme d'annotation dans une traduction par Albert Girard d'un traité d'arithmétique de Simon Stevin. Il est cependant généralement attribué à Fermat qui l'a précisé en spécifiant le nombre de façons différentes d'écrire un entier comme somme de deux carrés. Leonard Euler fut le premier à donner une preuve de ce résultat.

Démonstration (*du théorème de Fermat à partir du théorème de Don Quichotte*). Si le premier p appartient à $1 + 4\mathbf{N}$, alors $(p+1)/2$ est impair et l'involution

$$a \cdot b + c \cdot d \longmapsto b \cdot a + d \cdot c$$

agissant sur l'ensemble des $(p+1)/2$ écritures énumérées par le théorème de Don Quichotte a donc (au moins) un point fixe donné par $a = b > c = d$. ☐

Dans la suite, nous allons d'abord donner la liste des solutions pour les premiers impairs jusqu'à 29. Un dépliant décrit ensuite une construction naïve des solutions. Nous terminons avec une remarque sur la genèse du théorème de Don Quichotte. Le lecteur peut bien sûr continuer à donner sa préférence à la version de l'introduction.

Liste des solutions pour les premiers impairs

- Pour $p = 3$, les $(3+1)/2 = 2$ solutions sont

$$\begin{array}{c} 3 \cdot 1 + 0 \cdot 0 \\ 1 \cdot 3 + 0 \cdot 0 \end{array}$$

- Pour $p = 5$, les $(5+1)/2 = 3$ solutions sont

$$\begin{array}{c} 5 \cdot 1 + 0 \cdot 0 \\ 1 \cdot 5 + 0 \cdot 0 \\ 2 \cdot 2 + 1 \cdot 1 \end{array}$$

- Pour $p = 7$, les $(7+1)/2 = 4$ solutions sont

$$\begin{array}{c} 7 \cdot 1 + 0 \cdot 0 \\ 1 \cdot 7 + 0 \cdot 0 \\ 3 \cdot 2 + 1 \cdot 1 \\ 2 \cdot 3 + 1 \cdot 1 \end{array}$$

- Pour $p = 11$, les $(11+1)/2 = 6$ solutions sont

$$\begin{array}{c} 11 \cdot 1 + 0 \cdot 0 \\ 1 \cdot 11 + 0 \cdot 0 \\ 5 \cdot 2 + 1 \cdot 1 \\ 2 \cdot 5 + 1 \cdot 1 \\ 3 \cdot 3 + 2 \cdot 1 \\ 3 \cdot 3 + 1 \cdot 2 \end{array}$$

Pour avoir des listes plus courtes, on va supposer dorénavant $a \geqslant b > c \geqslant d$ en tenant compte des solutions oubliées par une multiplicité $\mu = \frac{1}{4} 2^{\sharp\{a,b,c,d\}}$, où $\sharp\{a,b,c,d\}$ désigne le cardinal de l'ensemble $\{a,b,c,d\}$. Cette multiplicté est donc égale à

- 1 si $a = b > c = d$;
- 2 si $a = b > c > d$ ou $a > b > c = d$;
- 4 dans les autres cas, c'est-à-dire si $a > b > c > d$.

On obtient ainsi

p	$a \cdot b + c \cdot d$	μ
13	$13 \cdot 1 + 0 \cdot 0$	2
	$6 \cdot 2 + 1 \cdot 1$	2
	$4 \cdot 3 + 1 \cdot 1$	2
	$3 \cdot 3 + 2 \cdot 2$	1
17	$17 \cdot 1 + 0 \cdot 0$	2
	$8 \cdot 2 + 1 \cdot 1$	2
	$4 \cdot 4 + 1 \cdot 1$	1
	$5 \cdot 3 + 2 \cdot 1$	4
19	$19 \cdot 1 + 0 \cdot 0$	2
	$9 \cdot 2 + 1 \cdot 1$	2
	$6 \cdot 3 + 1 \cdot 1$	2
	$4 \cdot 4 + 3 \cdot 1$	2
	$5 \cdot 3 + 2 \cdot 2$	2

p	$a \cdot b + c \cdot d$	μ
23	$23 \cdot 1 + 0 \cdot 0$	2
	$11 \cdot 2 + 1 \cdot 1$	2
	$7 \cdot 3 + 2 \cdot 1$	4
	$5 \cdot 4 + 3 \cdot 1$	4
29	$29 \cdot 1 + 0 \cdot 0$	2
	$14 \cdot 2 + 1 \cdot 1$	2
	$7 \cdot 4 + 1 \cdot 1$	2
	$9 \cdot 3 + 2 \cdot 1$	4
	$5 \cdot 5 + 4 \cdot 1$	2
	$5 \cdot 5 + 2 \cdot 2$	1
	$5 \cdot 4 + 3 \cdot 3$	2

pour les premiers $13, 17, 19, 23$ et 29. La dernière colonne donne la multiplicité (respectivement le nombre total de solutions donné par la somme des multiplicités) associée à la solution de la colonne du milieu. On se convaincra facilement en faisant quelques exemples supplémentaires de l'importance des factorisations des deux produits $a \cdot b$ et $c \cdot d$. Le théorème de Don Quichotte est donc peut-être un terrain de jeu ludique pour travailler des notions autour de la primalité et de la factorisation.

Construction élémentaire des solutions pour $p = 101$

Remarque finale

L'auteur de ce billet est tombé sur le théorème de Don Quichotte par pure sérendipité en étudiant une version matricielle de l'algorithme d'Euclide calculant le pgcd de deux entiers : la version la plus rudimentaire (fortement déconseillée quand les arguments sont grands) de l'algorithme consiste à itérer l'application

$$(a,b) \longmapsto (\max(a,b), \max(a,b) - \min(a,b))$$

pour a, b dans $\mathbf{N}$ jusqu'à stabilisation. Considérons une matrice carrée $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ avec A, B, C, D dans $\mathbf{N}$ et soustrayons une ligne ou une colonne de l'autre ligne ou colonne à condition de ne pas créer de coefficient strictement négatif. Cette opération préserve le déterminant $n = AD - BC$ (ainsi que le pgcd des quatre coefficients) et se termine avec une matrice satisfaisant $\min(A,D) > \max(B,C)$ si $n > 0$. Le nombre de telles matrices *irréductibles* de déterminant $n \geqslant 1$ donné est égal à

$$\sum_{d|n,\ d^2 \geqslant n} (d + 1 - n/d)$$

(voir [1] et la question [4]). Un changement de signe, fait par curiosité procrastinative, dans un programme très court écrit pour vérifier la formule ci-dessus dans les petits cas permet facilement de deviner le théorème de Don Quichotte (voir également la question [5]).

Références

[1] R. BACHER. « Euclid meets Popeye : The Euclidean Algorithm for 2 × 2 matrices ». *Comptes-rendus de l'Académie des sciences* 361 (2023), p. 889-895. DOI : `https://doi.org/10.5802/crmath.451`.

[2] Roland BACHER. « A Quixotic Proof of Fermat's Two Squares Theorem for Prime Numbers ». *The American Mathematical Monthly* 130.9 (2023), p. 824-836. DOI : `10.1080/00029890.2023.2242034`.

[3] M. de CERVANTES. *El ingenioso hidalgo don Quijote de la Mancha*. Madrid, 1605.

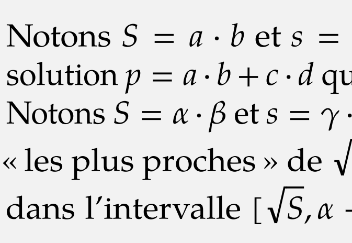
[4] MATHOVERFLOW. URL : `https://mathoverflow.net/questions/405035`.

[5] MATHOVERFLOW. URL : `https://mathoverflow.net/questions/405505`.

Remerciements

L'auteur et la rédaction d'Images des maths remercient Laurent Bartholdi et Sébastien Kernivinen pour leur relecture attentive.

Article édité par Jérôme Buzzi.



Roland BACHER
Maître de conférences – Université Grenoble-Alpes

Compléments

Construction élémentaire des solutions pour $p = 101$

Notons $S = a \cdot b$ et $s = c \cdot d$ les deux produits intervenant dans une solution $p = a \cdot b + c \cdot d$ que nous supposerons normalisée : $a \geqslant b > c \geqslant d$. Notons $S = \alpha \cdot \beta$ et $s = \gamma \cdot \delta$ avec $\alpha \geqslant \beta > \gamma \geqslant \delta$ les factorisations de S et s « les plus proches » de $\sqrt{S}$ et $\sqrt{s}$ dans le sens que S n'a pas de diviseur dans l'intervalle $[\sqrt{S}, \alpha - 1]$ et s n'a pas de diviseur dans l'intervalle $[\sqrt{s}, \gamma - 1]$. On a alors $a \geqslant \alpha \geqslant \sqrt{S} \geqslant \beta \geqslant b > c \geqslant \gamma \geqslant \sqrt{s} \geqslant \delta \geqslant d$. En cherchant pour $S + s = p$ donné les factorisations $S = \alpha\beta$ et $s = \gamma\delta$, on trouve facilement toutes les solutions.

Nous illustrons cette approche naïve en l'appliquant au premier $p = 101$. La deuxième colonne de la liste ci-dessous donne les factorisations $S = \alpha \cdot \beta$ et $s = \gamma \cdot \delta$ les plus proches de $\sqrt{S}$ et $\sqrt{s}$. Un couple $S + s = p$ avec $S > s$ ne contribue rien aux solutions si $\beta \leqslant \gamma$ et il contribue au moins avec la solution $\alpha \cdot \beta + \gamma \cdot \delta$ autrement. Toutes les solutions normalisées (par $a \geqslant b > c \geqslant d$) associées sont données dans la troisième colonne. La dernière colonne donne la multiplicité associée à la solution normalisée de la troisième colonne. La liste (légèrement tronquée) pour $p = 101$ est alors donnée par :

$S + s$	$\alpha \cdot \beta + \gamma \cdot \delta$	$a \cdot b + c \cdot d$	μ
$101 + 0$	$101 \cdot 1 + 0 \cdot 0$	$101 \cdot 1 + 0 \cdot 0$	2
$100 + 1$	$10 \cdot 10 + 1 \cdot 1$	$10 \cdot 10 + 1 \cdot 1$	1
		$20 \cdot 5 + 1 \cdot 1$	2
		$25 \cdot 4 + 1 \cdot 1$	2
		$50 \cdot 2 + 1 \cdot 1$	2
$99 + 2$	$11 \cdot 9 + 2 \cdot 1$	$11 \cdot 9 + 2 \cdot 1$	4
		$33 \cdot 3 + 2 \cdot 1$	4
$98 + 3$	$14 \cdot 7 + 3 \cdot 1$	$14 \cdot 7 + 3 \cdot 1$	4
$97 + 4$	$97 \cdot 1 + 2 \cdot 2$		
$96 + 5$	$12 \cdot 8 + 5 \cdot 1$	$12 \cdot 8 + 5 \cdot 1$	4
		$16 \cdot 6 + 5 \cdot 1$	4
$95 + 6$	$19 \cdot 5 + 3 \cdot 2$	$19 \cdot 5 + 3 \cdot 2$	4
$94 + 7$	$47 \cdot 2 + 7 \cdot 1$		
$93 + 8$	$31 \cdot 3 + 4 \cdot 2$		
$92 + 9$	$23 \cdot 4 + 3 \cdot 3$	$23 \cdot 4 + 3 \cdot 3$	2
$91 + 10$	$13 \cdot 7 + 5 \cdot 2$	$13 \cdot 7 + 5 \cdot 2$	4
$90 + 11$	$10 \cdot 9 + 11 \cdot 1$		
$89 + 12$	$89 \cdot 1 + 4 \cdot 3$		
$88 + 13$	$11 \cdot 8 + 13 \cdot 1$		
$87 + 14$	$29 \cdot 3 + 7 \cdot 2$		
$86 + 15$	$43 \cdot 2 + 5 \cdot 3$		
$85 + 16$	$17 \cdot 5 + 4 \cdot 4$	$17 \cdot 5 + 4 \cdot 4$	2
$84 + 17$	$12 \cdot 7 + 17 \cdot 1$		
$83 + 18$	$83 \cdot 1 + 6 \cdot 3$		
$82 + 19$	$41 \cdot 2 + 19 \cdot 1$		
$81 + 20$	$9 \cdot 9 + 5 \cdot 4$	$9 \cdot 9 + 5 \cdot 4$	2
$80 + 21$	$10 \cdot 8 + 7 \cdot 3$	$10 \cdot 8 + 7 \cdot 3$	4
$79 + 22$	$79 \cdot 1 + 11 \cdot 2$		
$78 + 23$	$13 \cdot 6 + 23 \cdot 1$		
$77 + 24$	$11 \cdot 7 + 6 \cdot 4$	$11 \cdot 7 + 6 \cdot 4$	4
$76 + 25$	$19 \cdot 4 + 5 \cdot 5$		
$75 + 26$	$15 \cdot 5 + 13 \cdot 2$		
$74 + 27$	$37 \cdot 2 + 9 \cdot 3$		
$73 + 28$	$73 \cdot 1 + 7 \cdot 4$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$52 + 49$	$13 \cdot 4 + 7 \cdot 7$		
$51 + 50$	$17 \cdot 3 + 10 \cdot 5$		

Le goulet d'étranglement de cette méthode est la nécessité de factoriser S et s. Ces factorisations deviennent coûteuses pour p très grand. On peut cependant s'inspirer de la preuve constructive (donnée dans [2]) du théorème de Don Quichotte pour établir de façon très différente la liste des solutions en utilisant $O(p \log p)$ opérations arithmétiques sur des entiers de taille au plus p.

Crédits

Frontispice : Louis Aquetin. *Don Quichote And Sancho Panza*. Aberdeen City Council (Archives, Gallery and Museums Collection).

---

[1] Certains esprits chagrins diront que les plaques de chocolat n'étaient pas connues à l'époque de Don Quichotte. Ce genre de calomnie ignoble ne mérite comme réponse qu'un proverbe cher à Sancho Panza : « La bave du crapaud n'atteint pas la blanche colombe ».

[2] Napoléon a bien son théorème. Ce n'est donc que justice que le plus grand des chevaliers errants ait le sien.

[3] Voir le début du chapitre 8 de la célèbre autobiographie de Don Quichotte écrite au noir par la fameuse plume de Cervantes [3].