18 décembre 2013 (rév. 24-12-2013)

Note sur la distribution des nombres premiers

Erika Lorena Álvarez Ramírez
Universidad Autónoma de la Ciudad de México,
Plantel Casa Libertad,
México, DF, Mexique

Jean Pestieau,
Université catholique de Louvain,
Institut de recherche en mathématique et physique (IRMP),
1348 Louvain-la-Neuve, Belgique

Les nombres premiers sont des nombres qui ne sont divisibles que par eux-mêmes et par l'unité. Par convention, 1 n'est pas un nombre premier. En dehors de 2 et de 5, tous les nombres premiers se terminent par 1, 3, 7 ou 9.

Prenons d'abord les premiers cent milles nombres premiers. Voici le nombre de nombres premiers se terminant par :

- 1 → 24 967
- 3 → 25 007
- 7 → 25 015
- 9 → 25 009

Prenons ensuite le premier million des nombres premiers. Voici le nombre de nombres premiers se terminant par :

- 1 → 249 934
- 3 → 250 110
- 7 → 250 014
- 9 → 249 940

Il n'y a rien qui privilégie à première vue les nombres premiers se terminant par soit 1, soit 3, soit 7 ou soit 9.[1] Cela se traduit par le fait que lorsque nous examinons les N premiers nombres premiers, nous avons que quand $N \to \infty$, le nombre de nombres premiers se terminant par 1, 3, 7 ou 9 tend, dans chaque cas, vers N/4.

Deux sortes de nombres premiers

Hormis 2, tous les nombres premiers sont impairs. Les nombres premiers impairs peuvent être divisés en deux groupes :

- ceux qui, lorsqu'ils sont divisés par 4, donnent un reste 1. Ils sont de la forme $4k + 1$ où k est n'importe quel nombre entier naturel.[2]
- ceux qui, lorsqu'ils sont divisés par 4, donnent un reste 3. Ils sont de la forme $4k + 3$.[3]

---

[1] Pour plus de précisions, voir Andrew Granville et Greg Martin, « Prime Number Races », *The American Mathematical Monthly*, vol. 113, no 1 (janvier 2006), p. 1-33, en ligne : http://www.dms.umontreal.ca/~andrew/PDF/PrimeRace.pdf.

[2] Ces nombres, hormis 5, doivent nécessairement se terminer par 01, 09, 13, 17, 21, 29, 33, 37, 41, 49, 53, 57, 61, 69, 73, 77, 81, 89, 93 ou 97.

[3] Ces nombres doivent nécessairement se terminer par 03, 07, 11, 19, 23, 27, 31, 39, 43, 47, 51, 59, 63, 67, 71, 79, 83, 87, 91 ou 99.

Prenons d'abord les premiers cent mille nombres premiers. Voici le nombre de nombres premiers, hormis 2, qui sont de la forme :

- $4k + 1 \rightarrow 49\,949$
- $4k + 3 \rightarrow 50\,050$

Prenons ensuite le premier million de nombres premiers. Voici le nombre de nombres premiers, hormis 2, qui sont de la forme :

- $4k + 1 \rightarrow 499\,798$
- $4k + 3 \rightarrow 500\,201$

Il n'y a rien qui semble privilégier les nombres premiers de la forme $4k + 1$ par rapport aux nombres premiers de la forme $4k + 3$.[4] Cela se traduit par le fait que lorsque nous examinons les N premiers nombres premiers, nous avons que quand $N \rightarrow \infty$, le nombre de nombres premiers de la forme $4k + 1$ tend vers N/2, tout comme ceux qui ont la forme 4k + 3.

Pour plus de détails, voir l'appendice.

Nous sommes en position de présenter le **théorème des deux carrés de Fermat**. Selon le théorème des deux carrés de Fermat[5] (appliqué au cas des nombres premiers), un nombre premier impair (c'est-à-dire tous les nombres premiers sauf 2) est une somme de deux carrés de nombres entiers naturels si et seulement si le reste de sa division par 4 est 1. Et, de plus, cette décomposition doit être unique.

Dit plus précisément, soit p un nombre premier impair, p est somme de deux carrés d'entiers naturels si et seulement si p est congru à 1 modulo 4 :

$$p = (2r)^2 + (2s - 1)^2$$

avec r et s deux entiers naturels. De plus, cette décomposition doit être unique. Dire que p est congru à 1 modulo 4 signifie que le reste de la division euclidienne de p par 4 est 1, ou encore que le nombre p est de la forme $4k + 1$.

Un nombre premier impair, si le reste de sa division par 4 est 3, ne peut jamais être exprimé comme la somme de deux carrés de nombres entiers naturels. Ainsi, nous avons

$5 = 1^2 + 2^2$,	$13 = 2^2 + 3^2$,	$17 = 1^2 + 4^2$,
$29 = 2^2 + 5^2$,	$37 = 1^2 + 6^2$,	$41 = 4^2 + 5^2$.

Par contre, 3, 7, 11, 19, 23, 31, 43 ne se décomposent pas ainsi.

À noter que

- $2 = 1^2 + 1^2$;
- 221 ne peut être un nombre premier puisque $221 = 5^2 + 14^2 = 10^2 + 11^2$;
- idem pour 493 puisque $493 = 3^2 + 22^2 = 13^2 + 18^2$, etc.

(nombre pair)² + (nombre impair)² et distribution des nombres premiers

Nous considérons les nombres naturels impairs de la forme

$$t = (2r)^2 + (2s - 1)^2 \qquad (1)$$

où r et s sont des nombres entiers naturels : 1, 2, 3, 4…

[4] Voir note 1.

[5] Dans le cas général, le théorème des deux carrés s'énonce comme suit : un entier naturel est somme de deux carrés si et seulement si chacun de ses facteurs premiers de la forme $4k + 3$ intervient à une puissance paire.

A. Soit l'ensemble des paires (r,s) qui par l'Éq. (1) donnent des t plus petits ou égaux à x, un nombre entier naturel quelconque. Nous appelons $M(x)$ le nombre de telles paires (r,s). Nous avons obtenu:

- pour $x = 100$, $M(x) = 17$[6]
- pour $x = 1\,000$, $M(x) = 188$
- pour $x = 10\,000$, $M(x) = 1\,939$
- pour $x = 100\,000$, $M(x) = 19\,559$
- pour $x = 1\,000\,000$, $M(x) = 196\,093$
- pour $x = 10\,000\,000$, $M(x) = 1\,962\,716$

Pour plus de détails, voir Tableau I.

Quand $x \to \infty$, nous avons[7] que

$$M(x) = (\pi/16) \times x. \tag{2}$$

Une meilleure approximation est donnée par[8]

$$M(x) = (\pi/16) \times x - 1/4 \times x^{1/2}.$$

B. Soit le nombre de t distincts, satisfaisant l'Éq. (1), qui sont inférieurs ou égaux à x. Nous appelons $N(x)$ le nombre de tels t. Nous avons obtenu :

- pour $x = 100$, $N(x) = 15$[9]
- pour $x = 1\,000$, $N(x) = 143$
- pour $x = 10\,000$, $N(x) = 1\,280$
- pour $x = 100\,000$, $N(x) = 11\,498$
- pour $x = 1\,000\,000$, $N(x) = 104\,701$

Pour plus de détails, voir Tableau II

Quand $x \to \infty$, nous avons que

$$N(x) = c \times x/(\ln x)^{1/2} \tag{3}$$

selon un théorème dû à Landau[10], avec c une constante.

Dans la même limite, nous pouvons remplacer l'Éq. (2) par

$$N(x) = c \times x^{1/2}\pi(x)^{1/2} \tag{4}$$

où $\pi(x)$ est le nombre de nombres premiers plus petits ou égaux à x. La constante c est de l'ordre de 0.37

---

[6] $M(100) = 17$ qui comprend : $1^2 + 2^2 = 5$, $1^2 + 4^2 = 17$, $1^2 + 6^2 = 37$, $1^2 + 8^2 = 65$, $3^2 + 2^2 = 13$, $3^2 + 4^2 = 25$, $3^2 + 6^2 = 45$, $3^2 + 8^2 = 73$, $5^2 + 2^2 = 29$, $5^2 + 4^2 = 41$, $5^2 + 6^2 = 61$, $5^2 + 8^2 = 89$, $7^2 + 2^2 = 53$, $7^2 + 4^2 = 65$, $7^2 + 6^2 = 85$, $9^2 + 2^2 = 85$, $9^2 + 4^2 = 97$.

[7] Nous remercions Andrew Granville de nous avoir signalé cette relation simple.

[8] Il est bon de noter les excellentes approximations suivantes :

$M(x) = (\pi/16) \times x - 1/4 \times x^{1/2}$, avec $M(x) = (\text{pairs})^2 + (\text{impair})^2 \leq x$.

$L(x) = (\pi/16) \times x - 1/2 \times x^{1/2}$, avec $L(x) = (\text{pairs})^2 + (\text{pairs})^2 \leq x$.

$K(x) = (\pi/16) \times x$, avec $K(x) = (\text{impairs})^2 + (\text{impairs})^2 \leq x$, avec pairs et impairs désignant les nombres naturels correspondants.

$1/2\,[L(x) + K(x)] = (\pi/16) \times x - 1/4 \times x^{1/2}$.

[9] $N(100) = 15$ qui comprend : 5, 13, 17, 25, 29, 37, 41, 45, 53, 61, 65, 73, 85, 89, 97.

[10] Voir note 7.

C. Soit le nombre de t distincts, satisfaisant l'Éq. (1), qui sont inférieurs ou égaux à x et tel qu'à un t donné ne correspond qu'une seule paire (r,s). Nous appelons $P(x)$ le nombre de tels t. Nous avons obtenu :

- pour $x = 100$, $P(x) = 13$[11]
- pour $x = 1\,000$, $P(x) = 103$
- pour $x = 10\,000$, $P(x) = 777$
- pour $x = 100\,000$, $P(x) = 5\,993$
- pour $x = 1\,000\,000$, $P(x) = 48\,360$

Pour plus de détails, voir Tableau III.

Comparons les $P(x)$ avec les $\pi(x)$ ainsi qu'avec $\pi(4k + 1\,;\, x)$, le nombre de nombres premiers de la forme $4k + 1$, plus petits ou égaux à x. Ainsi,

- pour $x = 100$, $\pi(x) = 25$ $\pi(4k + 1\,;\, x) = 11$
- pour $x = 1\,000$, $\pi(x) = 168$ $\pi(4k + 1\,;\, x) = 80$
- pour $x = 10\,000$, $\pi(x) = 1\,229$ $\pi(4k + 1\,;\, x) = 609$
- pour $x = 100\,000$, $\pi(x) = 9\,592$ $\pi(4k + 1\,;\, x) = 4\,782$
- pour $x = 1\,000\,000$, $\pi(x) = 78\,498$
- pour $x = 10\,000\,000$, $\pi(x) = 664\,579$

nous obtenons

- pour $x = 100$, $\pi(x)/2P(x) = 0.9615$ $\pi(4k + 1\,;\, x)/P(x) = 0.8462$
- pour $x = 1\,000$, $\pi(x)/2P(x) = 0.8155$ $\pi(4k + 1\,;\, x)/P(x) = 0.7767$
- pour $x = 10\,000$, $\pi(x)/2P(x) = 0.7909$ $\pi(4k + 1\,;\, x)/P(x) = 0.7838$
- pour $x = 100\,000$, $\pi(x)/2P(x) = 0.7996$ $\pi(4k + 1\,;\, x)/P(x) = 0.7981$
- pour $x = 1\,000\,000$, $\pi(x)/2P(x) = 0.8116$

Nous voyons la constance approximative du rapport entre $\pi(x)$ et $P(x)$ lorsque $1\,000 < x < 1\,000\,000$. Nous voudrions voir si cette constance se maintient pour $x > 1\,000\,000$. Si c'était le cas, nous aurions alors que $\pi(x)/2P(x)$ serait de l'ordre de 0.8 quand $x \to \infty$.

Nous conjecturons donc que

$$P(x) = \mathrm{a} \times \pi(x) \tag{5}$$

quand $x \to \infty$.

Des Éqs. (2), (4) et (5), nous obtenons alors dans la même limite,

$$N(x)/M(x) = (16\mathrm{c}/\pi)\pi(x)^{1/2} / x^{1/2}\ ;$$
$$P(x)/N(x) = (\mathrm{a}/\mathrm{c})\pi(x)^{1/2} / x^{1/2}.$$

[11] P(100) = 13 qui comprend : 5, 13, 17, 25, 29, 37, 41, 45, 53, 61, 73, 89, 97.

Tableaux I, II et III

Les tableaux ci-dessous indiquent les valeurs de M(x), N(x) et P(x) pour des valeurs de n égales à 100, 1 000, 100 000, 1 000 000. Elles sont ventilées entre les différents t [voir Éq.(1)] qui se terminent par les deux chiffres donnés dans la colonne à l'extrême-gauche des trois tableaux [voir la note 2].

I

	M(x), x =					
t	100	1 000	10 000	100 000	1 000 000	10 000 000
01	0	7	59	622	6 255	62 771
05	1	11	127	1 257	12 577	125 653
09	0	6	60	622	6 261	62 774
13	1	4	60	621	6 290	62 839
17	1	4	60	621	6 287	62 839
21	0	5	61	622	6 267	62 769
25	1	18	199	2 026	20 355	204 052
29	1	6	60	623	6 259	62 772
33	0	7	65	632	6 274	62 814
37	1	5	60	629	6 285	62 840
41	1	6	61	622	6 264	62 763
45	1	13	125	1 258	12 566	125 667
49	0	6	61	622	6 263	62 770
53	1	6	62	628	6 286	62 839
57	0	7	64	632	6 277	62 827
61	1	5	60	621	6 264	62 768
65	2	14	128	1 256	12 564	125 680
69	0	5	61	622	6 266	62 755
73	1	6	64	630	6 288	62 845
77	0	8	65	633	6 276	62816
81	0	6	62	622	6 269	62 774
85	2	14	124	1 258	12 572	125 666
89	1	5	61	619	6 266	62 765
93	0	7	65	631	6 278	62 820
97	1	7	65	630	6 284	62 838
	17	188	1 939	19 559	196 093	1 962 716

II

	N(x), x =				
t	100	1 000	10 000	100 000	1 000 000
01	0	6	46	448	4 110
05	1	7	57	493	4 408
09	0	6	48	444	4 112
13	1	4	49	451	4 125
17	1	4	47	451	4 134
21	0	4	52	450	4 105
25	1	8	66	552	4 834
29	1	5	49	451	4 095
33	0	6	52	452	4 119
37	1	5	50	454	4 122
41	1	6	48	444	4 107
45	1	7	56	490	4 402
49	0	5	49	446	4 112
53	1	6	49	452	4 130
57	0	7	51	452	4 120
61	1	5	47	445	4 119
65	1	7	57	487	4 389
69	0	5	49	447	4 103
73	1	6	51	448	4 126
77	0	7	52	451	4 127
81	0	5	51	448	4 110
85	1	7	53	487	4 389
89	1	4	48	446	4 121
93	0	5	52	453	4 119
97	1	6	51	456	4 123
	15	143	1 280	11 498	104 761

III

	P(x), x =				
t	100	1 000	10 000	100 000	1 000 000
01	0	5	34	297	2 419
05	1	3	6	18	50
09	0	6	38	290	2 411
13	1	4	38	302	2 412
17	1	4	34	302	2 434
21	0	3	43	304	2 381
25	1	2	6	17	46
29	1	4	39	305	2 380
33	0	5	39	298	2 427
37	1	5	40	303	2 426
41	1	6	35	284	2 402
45	1	2	6	17	45
49	0	4	37	292	2 413
53	1	6	37	296	2 427
57	0	7	40	296	2 405
61	1	5	36	290	2 417
65	0	0	0	0	0
69	0	5	37	291	2 398
73	1	6	39	289	2 420
77	0	6	41	293	2 415
81	0	4	41	295	2 388
85	0	0	0	0	0
89	1	3	35	300	2 416
93	0	3	39	304	2 409
97	1	5	37	310	2 419
	13	103	777	5 993	48 360

Appendice

Prenons parmi les cent milles premiers nombres premiers :

- ceux de la forme $4k + 1$ se terminant par 1, 3, 7, 9 ; ils sont respectivement au nombre de 12 463, 12 475, 12 536, 12 474 ;
- ceux de la forme $4k + 3$, se terminant par 1, 3, 7, 9 ; ils sont respectivement au nombre de 12 504, 12 532, 12 479, 12 535.

Prenons parmi le premier million des nombres premiers :

- ceux de la forme $4k + 1$ se terminant par 1, 3, 7, 9 ; ils sont respectivement au nombre de 124 844, 125 036, 125 075, 124 872 ;
- ceux de la forme $4k + 3$ se terminant par 1, 3, 7, 9 ; ils sont respectivement au nombre de 125 090, 125 074, 124 939, 125 098.