L'Algorithme de Génération des Premiers

Jacques Bienvenu *

29 avril 2010

Résumé

Cet article décrit un algorithme qui propose un point de vue nouveau sur la génération des nombres premiers. On l'appellera *Algorithme de Génération des Premiers* ou AGP.

*Professeur de mathématiques et Docteur ès lettres. Courriel : jybienvenu@wanadoo.fr

1 Introduction

Voici un nouvel algorithme dont le but n'est pas comme le crible d'Eratosthène de trouver les nombres premiers, mais qui permet de mieux comprendre la manière dont ils se forment. On l'appellera *Algorithme de Génération des Premiers* ou AGP.

2 Du crible d'Eratosthène à l'AGP

Le fameux crible d'Eratosthène vieux de plus de 2000 ans sera néanmoins un excellent moyen de comparaison pour introduire l'AGP. Rappelons son principe. Il est basé sur le fait qu'un nombre entier est premier s'il n'est pas divisible par tous les nombres qui lui sont strictement inférieurs à l'exclusion de 1. Si on cherche par exemple les nombres premiers inférieurs à cent, on opère ainsi : on place les nombres de 2 à 100 dans un tableau. On entoure le nombre 2 qui est premier, puis on barre les multiples stricts de 2 du tableau. On entoure le plus petit nombre non barré qui est 3. 3 est premier puisqu'il n'est pas divisible par les nombres qui lui sont inférieurs et qui se résument à 2. On entoure le nombre 3 et on barre tous les multiples stricts de 3. Le plus petit nombre non barré est 5 qui est premier car il n'est divisible ni par 2 ni par 3, ni par 4, et ainsi de suite. On obtient par ce procédé tous les nombres premiers inférieurs à cent. Le crible nous fait toucher du doigt qu'un nombre est premier en fonction de ceux qui l'ont précédé. Ainsi 5 est premier en fonction de la non divisibilité par 2 ou par 3. Ce qui explique d'ailleurs le mal que l'on a pour trouver les grands nombres premiers. A titre de comparaison élémentaire, si un nombre est pair cela ne dépend pas des nombres pairs qui l'ont précédé. Pour autant, si le crible permet de trouver les nombres premiers, il n'a pas la vocation d'expliquer leur répartition. Tout au contraire, il met en évidence que les nombres premiers apparaissent dans le tableau dans une succession qui ne laisse deviner aucun ordre et aucune loi, et c'est bien ce problème qui a tant intrigué, voire fasciné, les mathématiciens depuis plus de 2000 ans.

Dans le remarquable livre de Gilles Godefroy *L'aventure des nombres*, nous avons eu l'attention attiré par un chapitre intitulé "Connaître un ensemble par son complémentaire″. Gilles Godefroy exprime d'abord l'idée qu'il est difficile d'exhiber des nombres premiers arbitraire-

ment grands alors qu'on peut obtenir sans peine des nombres composés aussi grands soient - ils. Gilles Godefroy poursuit « Nous voyons ici poindre une idée, implicite chez Euclide comme chez Cantor : *on peut étudier un ensemble au moyen de son complémentaire*, montrer l'existence d'objets qui jouissent de certaines propriétés en étudiant les objets qui n'ont pas ces propriétés. Le crible d'Eratosthène, qui exhibe les nombres premiers comme étant ceux qui ne sont pas composés reflète d'ailleurs cette dissymétrie.» [1]

En effet, le crible se contente d'éliminer les composés pour faire apparaître les premiers. Avant de présenter notre algorithme (AGP) qui se propose plus précisément d'étudier les propriétés des nombres composés pour connaître leur complémentaire, les premiers, passons une dernière fois "au crible" le fameux crible ! Quand on barre les multiples de trois on constate que des nombres ont déjà été barrés. Ce sont bien entendu les multiples communs à deux et à trois. Cette simple remarque met en évidence ceci : en prenant successivement tous les multiples des nombres premiers on décrit $\mathbb{N}$ tout entier, mais on ne réalise pas une partition de l'ensemble des entiers naturels $\mathbb{N}$. Ce sera l'une des différences essentielles entre le crible et l'AGP.

L'AGP réalise, lui, une partition de $\mathbb{N}$ ce qui offre un avantage considérable pour les problèmes de dénombrements. L'autre différence que nous allons bientôt constater est que dans le crible tous les nombres non premiers sont impitoyablement barrés. Dans l'AGP, au contraire les nombres non premiers sont tous écrits et jouent tous leur rôle dans la constitution de l'algorithme. Mais il est temps à présent de décrire l'AGP.

La première caractéristique de cet algorithme est d'abord d'utiliser le théorème fondamental de l'arithmétique qui dit que tout nombre entier s'écrit de manière unique comme produit de nombres premiers. Aucun résultat important sur les nombres premiers ne peut se dispenser de cette propriété essentielle. Ainsi le succès de la fonction zêta de Riemann dans l'étude de la répartition des nombres premiers, vient du fait qu'elle rend compte, dans sa définition même, de la décomposition des entiers en facteurs premiers.

Longueur d'un entier

La longueur d'un entier est le nombre de premiers qui entrent dans la décomposition de cet entier en produit de facteurs premiers.

Exemples : la décomposition de 12 contient trois facteurs premiers ($12 = 2 \times 2 \times 3$). Ainsi la longueur de 12 est 3. De même la longueur de 5 est 1.

1. Gilles Godefroy, *L'aventure des nombres*, Editions Odile Jacob, 1997, p.133.

Avec cette définition les nombres premiers deviennent les nombres entiers de longueur 1. Il semble que la notion de longueur ait existé sous la dénomination d'ordre que nous avons rencontré dans un ancien traité d'arithmétique d'Edouard Lucas [2]. Toutefois, l'ordre au sens de longueur n'a pas eu en arithmétique la même fortune que celle de l'ordre de multiplicité des facteurs premiers. Aussi, prendrons-nous le terme de longueur qui évite toute confusion.

Il est très facile d'exprimer le théorème fondamental de l'arithmétique en terme de longueur. En effet, appelons E_r l'ensemble des entiers de longueur r, pour tout entier r. Dire que tout nombre est produit de manière unique de nombres premiers se traduit en disant que $\mathbb{N}$ est la réunion des E_r, et que les E_r forment une partition de N puisque $E_i \cap E_j = \varnothing$ pour $i \neq j$.

E_1 est donc l'ensemble des nombres premiers. Mais c'est un ensemble qui se construit pas à pas comme on va le voir. 2 étant le plus petit nombre premier, observons que les ensembles E_r ont un plus petit élément qui est 2^r. C'est donc le plus petit nombre de longueur r.

Considérons à présent les intervalles I_r définis par : $I_r = [2^r; 2^{r+1}[$ pour tout entier r. Tout entier de cet intervalle est strictement inférieur au plus petit entier de longueur $r + 1$. Il en résulte que la longueur maximum des entiers de I_r est r. Cette longueur est atteinte par 2^r. Nous admettrons provisoirement que les longueurs des entiers de I_r prennent toutes les valeurs de 1 à r. Observons que les intervalles $I_r$forment une partition de N et que par conséquent il en est de même des ensembles $I_r \cap E_i$ lorsque i varie de 1 à r.

L'algorithme AGP consiste à écrire successivement ces ensembles en commençant par $r = 0$, l'algorithme commençant vraiment pour $r = 1$ puisque 1 n'est pas premier. Comme ces ensembles forment une partition de $\mathbb{N}$, nous allons être amenés à réécrire les nombres entiers selon notre loi algorithmique.

2. Edouard Lucas, *Théorie des nombres*, Gauthier-Villars,1891, réédition Jacques Gabay, 1991, p.382.

Longueurs des entiers						
Intervalles I_r	1	2	3	4	5	...
$I_o = [2^0 ; 2^1 [$	1					
$I_1 = [2^1 ; 2^2 [$	2 3					
$I_2 = [2^2 ; 2^3 [$	5 7	2×3 2×2				
$I_3 = [2^3 ; 2^4 [$	11 13	2×5 2×7 3×5 3×3	2×2×2 2×2×3			
$I_4 = [2^4 ; 2^5 [$	17 19 23 29 31	2×11 2×13 3×7 5×5	2×3×3 2×2×5 2×3×5 2×2×7 3×3×3	2×2×2×2 2×2×2×3		
$I_5 = [2^5 ; 2^6 [$	37 41 43 47 53 59 61	2×31 2×29 2×23 2×19 2×17 3×19 3×17 3×13 3×11 5×11 5×7 7×7	2×2×11 2×2×13 2×2×7 3×3×5 3×3×7 2×5×5	2×2×2×5 2×2×2×7 2×2×3×3 2×2×3×5 2×3×3×3	2×2×2×2×2 2×2×2×2×3	
...				**Générés par 2 ; 3 ; 5 ; 7 ; 11 et 13**	**Stabilisé à 5 entiers Générés par 2 ; 3 ; 5 et 7**	**Stabilisé à 2 entiers Générés par 2 et 3**

Tableau 1 : Algorithme de Génération des Premiers (AGP)

La première remarque est que l'algorithme peut être considéré comme un crible. Ainsi pour trouver les nombres premiers de I_4 il faut écrire tous les entiers de longueur 4, 3 et 2, puis on en déduit que les entiers de I_4 qui n'ont pas été recensés par ce crible sont ceux de longueur 1, c'est à dire les premiers. Certes, ce crible est moins commode pour le calcul que celui d'Eratosthène mais il est vraisemblable qu'il ne poserait pas de problème pour une programmation avec ordinateur. Mais l'intérêt de l'algorithme est ailleurs. Commençons par quelques observations. Chaque I_r contient 2^r éléments et l'intervalle suivant deux fois plus. I_r comporte exactement r longueurs d'entiers. Donc quand on passe d'un intervalle I_r au suivant, on augmente les longueurs de 1, et on obtient une nouvelle liste de nombres premiers. Le prix à payer pour gagner une longueur est donc de doubler le nombre de termes. Reportons nous au *Tableau* 1 de l'AGP et observons l'intervalle I_4 : chaque longueur de I_4 est engendré par des nombres premiers bien précis. La longueur 4 par 2 et 3 ; la longueur 3 par 2 ; 3 ; 5 ; 7, la longueur 2 par 2 ; 3 ; 5 ; 7 ; 11 ; 13. Les couleurs des cellules du *Tableau* 1 ci-dessus illustrent qu'il en est de même pour les longueurs 5 ; 4 ; 3 de I_5 et pour les longueurs 2 et 3 de I_3.

On pourrait présenter de manière imagée l'algorithme ainsi : chaque intervalle I_r est un train. La locomotive est représentée par les nouveaux nombres premiers ; les wagons sont formés à l'aide des anciens. Le wagon de queue du train I_4 est formé par les premiers de l'intervalle I_1 à savoir 2 et 3. De plus le wagon de queue comportera toujours deux éléments quelque soit l'intervalle (dans I_{1000} les nombres de longueur mille sont au nombre de 2). L'avant dernier wagon de I_4 (les nombres de longueur 3) est formé des premiers qui se trouvent dans I_1 et I_2. Le nombre d'entiers de ce wagon est cinq et on peut montrer qu'il est stabilisé. C'est-à-dire que le nombre d'entiers de l'avant dernier wagon (les entiers de longueur 4) du train suivant I_5 est aussi égal à cinq comme on peut l'observer sur le *Tableau* 1. Plus les trains sont longs plus il y a de wagons comportant un nombre stabilisé d'entiers. Ainsi on montre que dans I_{100} les trente-six derniers wagons ont un nombre d'entiers stabilisé (voir ci-dessous le théorème dit de « stabilisation »).

3 Les lois mathématiques de L'AGP

On donne ici une série de théorèmes qui expliquent le fonctionnement de l'AGP. Le théorème de « stabilisation » (théorème 4) nous paraît le plus important.

Soit l'intervalle $I_r = [2^r; 2^{r+1}[$. On désigne par $L_{r,m}$ les entiers de I_r de longueur m. L'entier m varie donc de 1 à r.

Théorème 1

A) Les nombres premiers q qui sont dans la décomposition des entiers de $L_{r,m}$ sont tels que $q < 2^{r-m+2}$.

B) Pour tout q premier vérifiant la condition $q < 2^{r-m+2}$ il existe au moins un entier de $L_{r,m}$, avec $2 \leq m \leq r$, qui contient q comme facteur.

Preuve A)

Si $q \geq 2^{r-m+2}$ alors $2^{m-1}q \geq 2^{r+1}$. Or $2^{m-1}q$ est le plus petit entier de longueur m qui contient q. Donc il n'y a aucun entier de $L_{r,m}$ contenant q. On a donc nécessairement $q < 2^{r-m+2}$.

Pour démontrer B nous avons besoin du lemme suivant :

Lemme

Pour tout réel $x \geq 2$ on peut toujours trouver un nombre premier compris entre x et $2x$.

Preuve

Rappelons que le postulat de Bertrand assure que pour tout entier $n > 1$ on peut toujours trouver un nombre premier compris entre n et $2n$. [3]

Soit x réel, $x \geq 2$ et $E(x)$ la partie entière de x. On a $E(x) > 1$ et d'après Bertrand il existe un nombre premier p tel que $E(x) < p < 2E(x)$ qui entraîne $E(x) + 1 \leq p < 2E(x)$. Comme $E(x) \leq x < E(x)+1$. On déduit $x < E(x)+1 \leq p < 2E(x) \leq 2x$ ce qui prouve notre assertion.

3. Le postulat conjecturé Joseph Bertrand en 1845 a été démontré pour la première fois en 1850 par Pafnouti Tchebychev. Une démonstration relativement simple a été publiée par Paul Erdös en 1932. Voir à ce sujet l'article de Wikipedia http ://fr.wikipedia.org/wiki/Postulat_de_Bertrand

Preuve B)

Soit $q < 2^{r-m+2}$. Si $2^{r-m+1} \leq q < 2^{r-m+2}$ alors $2^r \leq 2^{m-1}q < 2^{r-1}$. Donc pour $2 \leq m \leq r$ il existe bien au moins un entier de $L_{r,m}$ qui contient q comme facteur. Si $q < 2^{r-m+1}$alors $2^{r-m+1}/q > 1$ et $2^{r-m+2}/q > 2$. Donc d'après le Lemme précédent, il existe un nombre premier p entre $2^{r-m+2}/q$ et $2^{r-m+3}/q$. On en déduit pour $2 \leq m \leq r$ que $2^{m-2}pq$ est dans I_r et ce nombre est bien un entier de longueur m qui contient q comme facteur.

En d'autres termes les entiers de longueur m telle que $2 \leq m \leq r$ d'un intervalle I_r sont « engendrés » par tous les nombres premiers inférieurs ou égaux à ceux de l'intervalle I_{r-m+1}. (On dira que des nombres premiers engendrent une collection H de nombres entiers si tous ces premiers se trouvent dans la décomposition des entiers de H et s'il n'y en a pas d'autres).

Pour bien comprendre ce résultat il est utile de reprendre le tableau précédent de notre algorithme correspondant à l'intervalle $I_4 = [24\ ;\ 25[$:

Tableau 2			
$L_{4,1}$	$L_{4,2}$	$L_{4,3}$	$L_{4,4}$
17	2×11	$2 \times 3 \times 3$	$2 \times 2 \times 2 \times 2$
19	2×13	$2 \times 2 \times 5$	$2 \times 2 \times 2 \times 3$
23	3×7	$2 \times 3 \times 5$	
29	5×5	$2 \times 2 \times 7$	
31		$3 \times 3 \times 3$	

On a dit que les entiers de $L_{r,m}$ sont engendrés par les nombres premiers qui vérifient $q < 2^{r-m+2}$.

Donc en faisant $r = 4$ on a $L_{4,m}$ qui est engendré par les $q < 2^{6-m}$:

Pour $m = 4$ on a $L_{4,4}$ engendrés par les premiers $q < 2^2$ soit $q = 2$ et $q = 3$.

Pour $m = 3$ on a $L_{4,3}$ engendrés par les premiers $q < 23$ soit $q = 2, q = 3, q = 5$ et $q = 7$.

Pour $m = 2$ on a $L_{4,2}$ engendrés par les premiers $q < 24$ soit $q = 2$, $q = 3,\ q = 5$,

$q = 7,\ q = 11$ et $q = 13$.

Ce que l'on vérifie aisément avec le tableau de I_4.

Théorème 2

Les nombres premiers qui engendrent $L_{r,m}$ avec $2 \leq m \leq r$ sont les mêmes que ceux qui engendrent $L_{r+n,m+n}$, avec n entier relatif tel que $n \geq 2 - m$.

Preuve

Les premiers qui engendrent $L_{r,m}$ avec $2 \leq m \leq r$ sont les premiers q tels que $q < 2^{r-m+2}$. Les premiers qui engendrent $L_{r+n,m+n}$ avec $2 \leq m+n \leq r+n$ (qui équivaut à $n \geq 2-m$ sous l'hypothèse $2 \leq m \leq r$) sont les premiers tels que $q < 2^{r+n-(m+n)+2}$, c'est-à-dire $q < 2^{r-m+2}$. Ce sont donc les mêmes que ceux qui engendrent $L_{r,m}$.

Par exemple, on voit dans le *Tableau* 1 donnant le début de l'algorithme : les entiers de $L_{4,3}$ sont $2 \times 3 \times 3$; $2 \times 2 \times 5$; $2 \times 3 \times 5$; $2 \times 2 \times 7$; $3 \times 3 \times 3$, et ceux de $L_{3,2}$ sont 2×5 ; 2×7 ; 5×5 ; 3×3. Ces deux collections d'entiers sont engendrés par les mêmes premiers 2 ; 3 ; 5 et 7 tels que $q < 23$.

Théorème 3

Pour $m \geq \frac{(r+1)ln2}{ln3}$ tous les entiers de $L_{r,m}$ sont pairs.

Preuve

En effet, 3^m est le plus petit entier de longueur m qui n'est pas pair. Donc pour $3^m \geq 2^{r+1}$ tout entier de $L_{r,m}$ est pair, ce qui est vrai pour $m \geq \frac{(r+1)ln2}{ln3}$.

Théorème 4 (dit de "stabilisation")

Pour r entier et pour $m \geq \frac{(r+1)ln2}{ln3}$ on a $card(L_{r,m}) = card(L_{r+n,m+n})$ pour tout entier n.

Preuve

D'après le Théorème 3, pour $m \geq \frac{(r+1)ln2}{ln3}$ les entiers de $L_{r,m}$ sont pairs. Dans ce cas, on en déduit que pour tout n, $m+n \geq \frac{(r+1)ln2}{ln3} + n$. Comme $\frac{ln2}{ln3} < 1$ on a $n\frac{ln2}{ln3} < n$ et finalement $m+n \geq (r+n+1)\frac{ln2}{ln3}$ qui prouve toujours d'après le Théorème 3 que les entiers de $L_{r+n,m+n}$ sont pairs.

Montrons à présent que, lorsque les entiers de $L_{r,m}$ sont pairs, $card(L_{r,m}) = card(L_{r+1,m+1})$.

Si $q_1.q_2 \dots q_m$ est un élément de $L_{r,m}$ alors $2q_1.q_2 \dots q_m$ est dans $L_{r+1,m+1}$. Et si n' est un élément de $L_{r+1,m+1}$, comme il est pair, il est de la forme $2q'_1.q'_2 \dots q'_m$ et $q'_1.q'_2 \dots q'_m$ est élément de $L_{r,m}$. Donc les entiers de $L_{r+1,m+1}$ sont tous les entiers $2n$ tels que n soit entier de Lr, m.

On a donc $card(L_{r,m}) = card(L_{r+1,m+1})$.

On en déduit par itération : $card(L_{r,m}) = card(L_{r+n,m+n})$ pour tout entier n.

Par exemple pour I_{100} on trouve $m \geq (101)\frac{ln2}{ln3}$, soit $m \geq 64$. Il y a donc 36 longueurs d'entiers dans I_{100} dont le cardinal est stabilisé. En d'autres termes, pour employer l'image ferroviaire précédente, pour $r \geq 100$ les 36 derniers wagons d'entiers de I_r auront toujours le même cardinal.

Théorème 5

Pour $n \geq (r+1)\frac{ln2}{(ln3-ln2)}$ le nombre des entiers de $L_{r+n,1+n}$ se stabilise.

Preuve

En effet, un raisonnement analogue à celui des Théorèmes 3 et 4 conduit à la majoration $3^{n+1} \geq 2^{r+n+1}$ qui donne le résultat annoncé.

Théorème 6

Pour $m \geq (r+1)\frac{ln2}{ln(p)}$ il n'y a aucun entier dans $L_{r,m}$ dont tous les termes sont supérieurs ou égaux à p, un nombre premier.

Preuve

En effet, p^m est le plus petit entier de longueur m dont tous les facteurs sont supérieurs ou égaux à p. Donc pour $p^m \geq 2^{r+1}$, il n'y a aucun entier dans $L_{r,m}$ dont tous les facteurs premiers sont supérieurs ou égaux à p. Soit pour $m \geq (r+1)\frac{ln2}{ln(p)}$.

Remarque : si on désigne par m_0 le plus petit entier m qui vérifie la majoration précédente, on peut en déduire que pour $m < m_0$ il existe au moins un entier de $L_{r,m}$ dont tous les facteurs premiers sont supérieurs ou égaux à p.

À titre d'exemple plaçons-nous dans I_4. Pour $p = 5$ on trouve : $m \geq 2.15\dots$ ce qui donne $m = 3$ pour le plus petit entier vérifiant cette condition.

On se rapportera au *Tableau* 2 ci-dessus. Pour $m = 2$ on en déduit qu'il existe au moins un nombre dont tous les termes sont supérieurs ou égaux à 5, ce que confirme le nombre 5×5.

Toujours dans I_4 et pour $p = 7$ on trouve : $m \geq 1.78$ soit $m \geq 2$. Nous laissons au lecteur le soin de trouver ce qu'il en résulte pour m.

4 Conclusion : l'ordre plutôt que le chaos

L'AGP a permis de révéler une structure. Les intervalles I_r apparaissent dans cet algorithme comme la cellule de fabrication d'une collection de nombres premiers P_r qui n'interviennent jamais dans la formation des entiers de I_r et a fortiori dans les intervalles précédents. En revanche ils vont servir à engendrer les intervalles suivants : les entiers de longueur 2 de I_{r+1}, les entiers de longueur 3 de I_{r+2} et ainsi de suite jusqu'à une longueur n dont le cardinal va se stabiliser. Par ailleurs chaque intervalle I_r comprend exactement r longueurs d'entiers qui sont engendrés de r à 2 respectivement par $P_1; P_1 \cup P_2; ...; P_1 \cup P_2 \ldots \cup \ P_{r-1}$. Si bien que l'intervalle I_r apparaît aussi comme l'historique des nombres premiers construits avant lui. Il y a là un véritable mouvement d'horlogerie qui montre davantage l'ordre que le chaos. Si l'on considère la suite des nombres premiers donnés dans les tables, elle semble être régie par le hasard. Cela provient du fait, à notre avis, que la suite ordonnée des nombres entiers donne la priorité à la structure additive de $\mathbb{N}$. Dans notre algorithme qui donne la priorité à la structure multiplicative qui définit les nombres premiers, un ordre nouveau apparaît avec des lois d'une rigoureuse précision. On voit que ce n'est plus le nombre premier seul, qu'il faut considérer mais la collection de ceux qui sont contenus dans chaque intervalle I_r. Ramener l'étude des nombres premiers de $\mathbb{N}$ à ceux des intervalles I_r, telle est la voie que nous proposons. L'encadrement entre des puissances de deux est essentiel. Il suffit de construire un algorithme avec comme encadrement des puissances de trois pour constater qu'il n'offre pas d'intérêt. On voit aussi que l'algorithme offre des perspectives dans le domaine du dénombrement et du même coup on retrouve le grand problème de la répartition des nombres premiers. L'étude des entiers de longueur 2, mis en évidence dans l'AGP, concerne les problèmes de cryptographie. Les nombres premiers de Mersenne ont une place privilégiée dans l'AGP. En effet le plus grand nombre de chaque intervalle I_r est $2^{r+1} - 1$ et par conséquent tous les nombres premiers de Mersenne seront à cette place, ce qui n'est peut-être pas anodin. C'est sur ces perspectives que nous terminons cet article.

5 Bibliographie

Jacques Bienvenu, "L'algorithme de génération des premiers (AGP)", Revue Tangente, n°108, 2006

Chris Caldwell, Site Web "The primes pages", http ://primes.utm.edu/.
Un site fameux et très complet sur les nombres premiers.

Jean-Paul Delahaye, *Merveilleux nombres premiers. Voyage au cœur de l'arithmétique*, Éditions Belin/Pour la science, Paris, 2000.
Incontournable référence.

Gilles Godefroy, *L'aventure des nombres*, Editions Odile Jacob, 1997.
Une réflexion profonde sur la notion et l'histoire des nombres.

Andrew Grandville, "Nombres premiers et chaos quantique", 2002.
En ligne http ://smf4.emath.fr/Publications/Gazette/2003/97/smf_gazette_97_29-44.pdf
Cet article fascinant et accessible porte sur des recherches récentes.

Edouard Lucas, *Théorie des nombres*, Gauthier-Villars, 1891, réédition Jacques Gabay, 1991.
Ouvrage historiquement très intéressant dans lequel on observe que toutes les questions ouvertes sur les nombres premiers posées en 1891 n'ont toujours pas été résolues.

M. Mendes France, G. Tenenbaum, *Les nombres premiers*. Que sais-je ? vol. 571. Presses Universitaires de France, 1997.
Un classique.