La méthode générale du crible et sa place dans la théorie des nombres premiers

Atle Selberg

Depuis que Viggo Brun a introduit son ingénieuse méthode du crible, celle-ci est devenue un outil très important pour l'étude des problèmes de la théorie des nombres premiers. Cela est dû notamment à l'extrême généralité de la méthode, qui lui permet de donner des résultats là où les outils analytiques plus fins ne fonctionnent pas. Mais la méthode du crible est également caractérisée par le fait qu'elle ne conduit qu'à des résultats partiels et incomplets. De plus, l'obtention de bons résultats avec cette méthode nécessitait des calculs numériques assez importants en raison de sa complexité. Cette complexité a d'ailleurs augmenté à mesure que diverses améliorations techniques ont été apportées par plusieurs mathématiciens, parmi lesquels Rademacher, Estermann, Ricci et Buchstab.

Dans cette conférence, je parlerai d'une méthode du crible plus générale que j'étudie depuis quelques années.

Cette méthode inclut la méthode de Brun et ses améliorations comme cas particulier. Elle conduit à une formulation plus claire et plus simple des principaux problèmes liés à la méthode du crible, ce qui permet d'obtenir des informations sur les limites de la méthode. Il convient également de mentionner qu'elle conduit à de meilleurs résultats que la méthode de Brun.

1. Le problème auquel se rapporte la méthode du crible peut être formulé comme suit :

Nous avons un ensemble d'entiers n dont le nombre total est noté N, et un certain ensemble de nombres premiers $p_i, i = 1, 2, \ldots, r$, et nous voulons estimer le nombre de nombres n qui ne sont divisibles par aucun des nombres premiers p_i donnés [1].

Souvent, cela est énoncé sous une forme apparemment plus générale, où nous comptons les n qui ne sont pas congrus à un certain ensemble de résidus modulo chaque p_i.

Si l'on note $N(p_1, p_2, \ldots, p_r)$ le nombre de n qui ne sont divisibles par aucun p_i, on a, si d désigne dans ce qui suit les entiers positifs composés uniquement de nombres premiers p_i et $\mu(d)$ est la fonction de Möbius, que

$$N(p_1, \ldots, p_r) = \sum_n \sum_{d|n} \mu(d) = \sum_d \mu(d) \sum_{d|n} 1. \tag{1}$$

Référence : A. Selberg, *The general sieve method and its place in prime number theory*, Proc. Internat. Congress Math., Cambridge, Mass. 1950, vol. 1, p. 286-292, Amer. Math. Soc., 1952.
Transcription et traduction : Denise Vella-Chemla, juillet 2026.

1. On peut généraliser cela pour demander le nombre de nombres n qui ne contiennent pas plus de k facteurs premiers de l'ensemble donné des p_i, et les compter avec des poids dépendant de ces facteurs premiers. Ceci est souvent avantageux si l'on veut prouver qu'il existe des nombres d'un type donné avec un petit nombre de facteurs premiers. Par exemple, on peut prouver de cette manière que tout grand nombre pair peut être écrit comme la somme de deux nombres positifs, dont l'un contient au plus 2 facteurs premiers et l'autre au plus 3.

Supposons maintenant que nous ayons une expression approchée du nombre de nombres n divisibles par d, de la forme

$$\sum_{d|n} 1 = \frac{N}{f(d)} + R_d, \tag{2}$$

ici, $f(d)$ est une fonction multiplicative [2], et R_d est un terme de reste dont nous ne connaissons rien de plus qu'une borne supérieure pour $|R_d|$. À partir de (1), nous allons alors trouver,

$$\begin{aligned} N(p_1, \ldots, p_r) &= N \sum_d \frac{\mu(d)}{f(d)} + \theta \sum_d |R_d| \\ &= N \prod_{i=1}^{r} \left(1 - \frac{1}{f(p_i)}\right) + \theta \sum_d |R_d| \ , \end{aligned} \tag{3}$$

ici $-1 \leq \theta \leq 1$. L'inconvénient de (3), cependant, est que, sauf dans le cas presque trivial où r est très petit par rapport à N, le terme de reste sera beaucoup plus grand que le terme principal, de sorte que (3) n'est d'aucune utilité.

La méthode du crible est conçue pour remédier à cette difficulté. Elle est basée sur la considération suivante. Au lieu de déterminer $N(p_1, p_2, \ldots, p_r)$ directement, nous allons essayer de trouver des bornes supérieure et inférieure pour celui-ci en remplaçant l'expression $\sum_{d|n} \mu(d)$ apparaissant dans (1) par une expression construite de manière similaire à (1) et qui respectivement majore ou minore cette expression, et en même temps réduit le terme de reste à une taille raisonnable.

Ainsi, pour trouver une borne supérieure pour $N(p_1, \ldots, p_r)$, nous prenons un ensemble de nombres réels ρ_d avec $\rho_1 = 1$, et tel que pour tout entier n,

$$\sum_{d|n} \rho_d \geq \sum_{d|n} \mu(d) \ ; \tag{4}$$

alors nous obtenons une borne supérieure

$$N(p_1, \ldots, p_r) \leq N \sum_d \frac{\rho_d}{f(d)} + \sum_d |\rho_d| \ |R_d| \ . \tag{5}$$

Il reste alors le problème de déterminer les ρ qui satisfont (4) et rendent le membre de droite de (5) aussi petit que possible.

De même, si nous avons un ensemble de ρ_d avec $\rho_1 = 1$, et tel que pour tout entier n,

$$\sum_{d|n} \rho_d \leq \sum_{d|n} \mu(d), \tag{6}$$

2. C'est la forme qui apparaît généralement dans les applications. On peut également considérer des formes plus générales du terme dominant dans (2).

nous obtenons une borne inférieure

$$N(p_1, \dots, p_r) \geq N \sum_d \frac{\rho_d}{f(d)} + \sum_d |\rho_d| \, |R_d| \, , \tag{7}$$

Le problème consiste à choisir les ρ qui maximisent le membre de droite selon les conditions (6).

Les problèmes de recherche d'une borne supérieure et d'une borne inférieure pour $N(p_1, \dots, p_r)$ se réduisent à deux problèmes d'extremum, qui semblent malheureusement être très difficiles à résoudre. Par conséquent, nous devrons être satisfaits si, en introduisant davantage de restrictions sur les ρ, nous pouvons obtenir un nouveau problème de calcul d'extremum qui puisse être résolu. Cela impliquera, bien sûr, que notre résultat ne sera probablement pas le meilleur possible. Cependant, dans certains cas, nous pouvons effectivement obtenir les meilleurs résultats possibles.

2. Il faudrait trop de temps pour détailler les principes que nous pouvons utiliser avantageusement afin d'obtenir un problème d'extremum que nous pouvons résoudre et qui donne un bon résultat ; quelques indications suffiront donc.

Premièrement, si nous regardons le membre de droite de (5) ou (7), nous constatons que pour obtenir un bon résultat, le second terme $\sum_d |\rho_d| \, |R_d|$ ne doit pas être trop grand. Puisque, dans les cas les plus intéressants, les $|R_d|$ ne sont pas très grands, cela peut être obtenu en limitant la taille d'un $\sum_d |\rho_d|$ d'une manière appropriée. On peut essayer de l'obtenir en exigeant que, sauf pour un certain nombre d'entre eux, les ρ soient nuls, par exemple en prenant $\rho_d = 0$ pour $d > z$, où z est convenablement choisi, nous pouvons nous attendre à ce que $\sum_d |\rho_d|$ ne soit pas essentiellement supérieur à z en ordre de grandeur [3].

Vient ensuite le problème de la satisfaction des inégalités (4) ou (6). Pour (4), cela peut être fait de manière très simple en prenant un ensemble de nombres réels λ_d avec $\lambda_1 = 1$ et en posant

$$\rho_d = \sum_{d_1 d_2 / \kappa = d} \lambda_{d_1} \lambda_{d_2}, \qquad\qquad \kappa = (d_1, d_2) \tag{8}$$

Alors

$$\sum_{d|n} \rho_d = \{\sum_{d|n} \lambda_d\}^2 \geq \sum_{d|n} \mu(d),$$

de sorte que (4) soit satisfaite. Afin de rendre $\rho_d = 0$ pour $d > z$, nous exigeons que $\lambda_d = 0$ pour $d > z^{1/2}$. Il reste alors à rendre le premier terme du membre de droite de (5) aussi petit que possible. Ce terme prend la forme

$$N \sum_{d_1, d_2 \leq z^{1/2}} \frac{\lambda_{d_1} \lambda_{d_2}}{f(d_1) f(d_2)} f(\kappa), \tag{9}$$

3. Cela peut en fait être prouvé comme étant le cas si $\sum_d \rho_d / f(d)$ est petit et que les ρ satisfont soit (4), soit (6).

et notre problème consiste maintenant simplement à trouver le minimum de cette expression sous la condition $\lambda_1 = 1$. Cela peut être facilement fait, le minimum étant

$$\frac{N}{\sum\limits_{d \le z^{1/2}} \dfrac{\mu^2(d)}{f'(d)}}, \tag{10}$$

où

$$f'(d) = f(d) \prod_{p|d} \left(1 - \frac{1}{f(p)}\right).$$

Si z est alors choisi de manière appropriée, le terme $\sum\limits_d |\rho_d|\ |R_d|$ devient suffisamment petit par rapport à (10) pour nous donner une bonne borne supérieure (5).

Le cas de la borne inférieure est essentiellement plus compliqué car il n'est pas aussi simple de satisfaire les inégalités (6) que les inégalités (4).

Une façon de procéder consiste, par exemple, à écrire

$$\rho_d = - \sum_{d_1 d_2 = \kappa d,\ p|\mu} \lambda_{d_1} \lambda_{d_2},$$

où p est le plus grand nombre premier divisant d, et à prendre $\lambda_p = 1$ pour tout p. Alors (6) est automatiquement satisfait. De plus, si nous contraignons λ_d à être $= 0$ pour $d > (zp)^{1/2}$ où p est le plus grand nombre premier divisant d, nous avons $\rho_d = 0$ pour $d > z$. Nous devons alors déterminer le maximum du premier terme du membre de droite de (7). Cela peut effectivement être fait, mais c'est considérablement plus compliqué que dans le cas précédent. Il existe également des méthodes alternatives, qui impliquent cependant toutes des calculs assez importants si l'on essaie d'obtenir un bon résultat.

Enfin, il convient de mentionner qu'il existe certains principes qui, dans de nombreux cas, permettent d'améliorer progressivement les résultats obtenus pour la borne supérieure ou inférieure par les méthodes mentionnées précédemment. Malheureusement, cette procédure nécessite également des calculs assez importants dans la plupart des cas.

Les résultats obtenus par ces méthodes sont meilleurs que ceux obtenus par la méthode classique du crible, mais dans la plupart des cas, ils ne représentent certainement pas le meilleur résultat possible puisque nous avons soumis nos ρ à des restrictions assez sévères afin d'obtenir un problème d'extremum que nous pouvions résoudre.

3. Tant que nous ne pouvons pas résoudre les problèmes d'extremum liés à la méthode du crible sous leur forme générale, il est intéressant d'avoir des bornes pour ces valeurs extrémales. De telles bornes dans une direction sont bien sûr données par les résultats obtenus pour les problèmes d'extremum restreints. Mais pour les cas les plus intéressants pour la théorie des nombres, par exemple

lorsque les nombres n sont les valeurs prises par un polynôme à valeurs entières $P(x)$ sans diviseurs premiers fixes lorsque l'argument x parcourt N entiers consécutifs, et que l'ensemble des nombres premiers $p_1, \ldots, p_r$ est l'ensemble de tous les nombres premiers inférieurs à un certain nombre ξ, nous pouvons prouver des résultats intéressants dans l'autre direction. Autrement dit, nous pouvons donner des bornes qu'aucun résultat obtenu par la méthode du crible ne peut surpasser. En particulier, ces résultats montrent que pour certains problèmes qui ont été attaqués à plusieurs reprises au moyen de la méthode du crible, une solution de cette manière est certainement impossible. Ils montrent également, ce qui est plus surprenant encore, que dans certains cas particuliers, les résultats obtenus par les méthodes expliquées au § 2 sont en fait les meilleurs résultats possibles.

La raison pour laquelle la méthode du crible ne peut pas donner de "trop bons" résultats est qu'elle n'est pas très sensible à l'ordre de grandeur des termes de reste R_d dans un certain sens, par exemple, si nous avons $n = P(x)$ lorsque x parcourt N entiers successifs et $P(x)$ est un polynôme à valeurs entières sans diviseurs premiers fixes. Dans ce cas, si $u(d)$ désigne le nombre de solutions de la congruence $P(x) = 0 \pmod{d}$, nous avons $1/f(d) = u(d)/d$, et pour R_d, nous avons le résultat $|R_d| \leq u(d)$. Cependant, nous obtenons essentiellement les mêmes résultats par la méthode du crible, si nous supposons seulement que

$$R_d = \mathrm{O}\left(\frac{u(d)N}{d(\log\,(N/d))^k}\right),$$

pour un exposant k suffisamment élevé qui dépend du nombre de facteurs irréductibles en lesquels $P(x)$ peut être factorisé. Cette remarque permet de remplacer le problème initial par un problème essentiellement équivalent par rapport à la méthode du crible, mais pour lequel nous essayons de rendre le $N(p_1, \ldots, p_r)$ aussi grand ou aussi petit que possible, et ainsi obtenir des résultats du type souhaité.

Considérons par exemple le cas simple où les nombres n sont N entiers consécutifs, et essayons d'estimer une borne supérieure du nombre de ces entiers qui n'ont pas de facteur premier inférieur à $\xi = N^\alpha$ où $0 < \alpha < 1$. Nous écrivons pour abréger $N(\xi)$ au lieu de $N(p_1, \ldots, p_r)$. Dans ce cas, nous avons $f(d) = d$ et $|R_d| \leq 1$ de sorte que (5) prend la forme

$$N(\xi) \leq N \sum_d \frac{\rho_d}{d} + \sum_d |\rho_d|. \tag{11}$$

La méthode expliquée au § 2 donne très facilement une borne supérieure de la forme $\mathrm{O}(N/\log N)$, ce qui nous permet de nous limiter au cas où :

$$\sum_d \frac{\rho_d}{d} = \mathrm{O}\left(\frac{1}{\log N}\right), \qquad \sum_d |\rho_d| = \mathrm{O}\left(\frac{N}{\log N}\right). \tag{12}$$

De ceci et (4), on peut déduire

$$\sum_d \frac{|\rho_d|}{d} = \mathrm{O}(\log N). \tag{12'}$$

Maintenant, si l'on considère l'ensemble de tous les entiers positifs $n' \leq N$, avec un nombre impair de facteurs premiers, on a

$$\sum_{d \,|\, n'} 1 = \frac{N}{2d} + \mathrm{O}\left(\frac{N}{d} e^{-(\log (N/d))^{1/2}}\right),$$

en vertu d'un résultat bien connu de la théorie analytique des nombres. Ainsi, si l'on applique notre crible à cet ensemble de nombres n', et que l'on note $N'(\xi)$ le nombre de ceux qui n'ont pas de facteur premier $\leq \xi$, on obtient

$$2N'(\xi) \leq N \sum_d \frac{\rho_d}{d} + \mathrm{O}\left(N \sum_d \frac{|\rho_d|}{d} e^{-(\log(N/d))^{1/2}}\right). \tag{13}$$

Cependant, nous ne pouvons pas être sûrs ici que le terme de reste soit suffisamment petit par rapport au terme principal, de sorte que nous ne pouvons pas tirer de conclusions immédiates de (13). Cela change si nous remplaçons N ici par un nombre un peu plus grand, par exemple par $N_1 = N^{1+\epsilon}$ où $\epsilon > 0$ tend vers zéro d'une manière appropriée lorsque N tend vers l'infini, alors (12) et (12') suffisent à rendre le terme de reste suffisamment petit. De cela, nous pouvons tirer des conclusions qui nous donnent une borne inférieure pour $\sum_d \rho_d/d$, et ainsi, une borne inférieure pour la borne supérieure de $N(\xi)$ que nous pouvons obtenir à partir de (11). Le résultat est que nous ne pouvons pas obtenir une borne supérieure inférieure à

$$2N'(\xi) - \mathrm{O}\left(N \left(\frac{\log\log N}{\log N}\right)^2\right) \tag{14}$$

De la même manière, nous pouvons prouver qu'une borne inférieure obtenue par la méthode du crible ne peut pas être supérieure à

$$2N''(\xi) + \mathrm{O}\left(N \left(\frac{\log\log N}{\log N}\right)^2\right). \tag{14'}$$

Ici, $N''(\xi)$ dénote le nombre d'entiers positifs $\leq N$ avec un nombre pair de facteurs premiers et aucun facteur premier $\leq \xi$. Si on prend $\alpha = 1/2$; $\xi = N^{1/2}$, on a

$$N'(\xi) = \pi(N) - \pi(N^{1/2}) = \frac{N}{\log N} + \mathrm{O}\left(\frac{N}{\log^2 N}\right),$$

et

$$N''(\xi) = 1$$

Donc (14) donne

$$\frac{2N}{\log N} - \mathrm{O}\left(N \left(\frac{\log\log N}{\log N}\right)^2\right)$$

comme borne inférieure pour la borne supérieure. Avec la méthode décrite au § 2, nous pouvons réellement obtenir la borne supérieure

$$\frac{2N}{\log N} + \mathrm{O}\left(\frac{N}{\log^2 N}\right),$$

qui est par conséquent essentiellement le meilleur résultat possible. (14') devient

$$O\left(N\left(\frac{\log\log N}{\log N}\right)^2\right)$$

Par conséquent, la méthode du crible ne peut pas donner le bon ordre de grandeur pour le nombre de nombres premiers $\leq N$. Pour $1/2 < \alpha < 1$, nous pouvons même prouver que la borne inférieure est négative pour les grands N [4]. Si nous laissons α diminuer de $1/2$ à 0, nous voyons que $N'(\xi)$ et $N''(\xi)$ diffèrent de moins en moins. Ceci concorde avec le fait que la méthode du crible fonctionne mieux pour les petits exposants α.

Nous ne pouvons pas prouver que les bornes données par (14) et (14') représentent essentiellement les vraies limites de ce qui peut être obtenu par la méthode du crible. Cependant, par les méthodes expliquées au § 2, on peut s'en approcher très près. Un intérêt particulier est porté à la valeur de l'exposant α, lorsque la borne inférieure cesse d'être positive et devient négative à mesure que α augmente. Nous pouvons appeler cela la limite de criblage du problème.

D'après ce qui précède, nous avons que la limite de criblage dans ce cas est $\leq 1/??$. Par les méthodes du § 2, nous pouvons très facilement montrer qu'elle est également $> 0,465$, une valeur qui peut être améliorée étape par étape par des calculs supplémentaires. Je ne sais pas si cette procédure convergerait réellement vers $1/2$.

Cette analyse peut facilement être étendue au cas où les nombres n sont les valeurs d'un polynôme irréductible à valeurs entières $P(x)$ sans diviseur premier fixe lorsque x parcourt N entiers successifs, avec essentiellement les mêmes résultats.

Dans le cas des polynômes réductibles, nous pouvons prouver des résultats similaires, mais il existe un plus grand écart entre ces résultats et les bornes réellement obtenues par les méthodes du § 2. Un cas particulièrement intéressant est celui du polynôme composé de deux facteurs irréductibles, qui comprend deux problèmes bien connus qui ont été attaqués à plusieurs reprises au moyen de la méthode du crible, à savoir le problème de l'infinité des nombres premiers jumeaux et le problème de Goldbach.

La première solution correspond à prendre le polynôme $x(x+2)$ pour $x = 1, 2, \ldots, N$ et $\xi = (N+2)^{1/2}$. Si nous pouvions alors obtenir une borne inférieure positive, le problème serait résolu. Cependant, nous pouvons démontrer que pour $\xi = N^\alpha$, la borne inférieure est en réalité négative pour les grandes valeurs de N si $\alpha > 1/(1+e^{3/4})$ [5], ce qui empêche la méthode du crible de résoudre ce problème. Le résultat correspondant est valable pour le problème de Goldbach et, plus généralement, pour le cas d'un polynôme à deux facteurs irréductibles. Nous pouvons également montrer qu'il existe des limitations similaires pour les bornes supérieures obtenues par la méthode du crible, mais dans ce cas, l'écart entre ces résultats et ceux obtenus par les méthodes du § 2 est plus important. Nous pouvons montrer, par exemple, que la meilleure borne supérieure obtenue

4. Ceci est vraiment dû au fait que nous avons exigé que ρ_1 soit égal à 1. Si nous demandons seulement que $\rho_1 \leq 1$, la borne inférieure ne peut jamais devenir négative, puisque nous pouvons prendre tous les ρ_d égaux à 0. Cependant, si la borne inférieure est positive, elle sera atteinte avec un ensemble de ρ tels que $\rho_1 = 1$.

5. Ce nombre peut en fait être remplacé par un nombre légèrement plus petit.

pour le nombre de nombres premiers jumeaux $\leq N$ est, pour les grandes valeurs de N, plus de quatre fois supérieure[6] à la valeur asymptotique généralement admise[7]. Par la méthode décrite au § 2, nous obtenons en réalité une borne huit fois trop grande. Je suis enclin à penser que, dans les faits, il s'agit de la meilleure borne possible.

4. Compte tenu de cela, il semble que la méthode du crible sera de peu d'utilité pour la poursuite des progrès de ces problèmes de la théorie des nombres premiers pour lesquels elle a été initialement conçue. Mais elle reste un outil extrêmement général et polyvalent pour établir, par exemple, des bornes supérieures, et pourrait peut-être, combinée d'une manière ou d'une autre à une approche analytique, jouer un rôle important dans l'avenir de ces problèmes.

Institut des études avancées (IAS),
Princeton, New Jersey, États-Unis

6. Le facteur 4 peut être remplacé par un nombre légèrement plus grand.
7. Notamment $T(N) \sim kN/\log^2 N$ avec $k = 2\prod_{p\geq 3}(1 - 1/(p-1)^2) = 1,320\ldots$

18. Une digression historique, le principe de parité et un autre exemple [8]

En examinant les ensembles pondérés construits dans la section 16 afin de démontrer le théorème 13 et l'utilisation de la fonction de Liouville $\lambda(n)$, nous constatons que nous avons utilisé deux faits essentiels :

(1) Les entiers $1 \leq n \leq x$ sont, pour de grandes valeurs de x, assez uniformément répartis entre la classe des nombres avec $\lambda(n) = 1$ (ou avec $\nu(n)$ pair) et la classe des n avec $\lambda(n) = -1$ (ou avec $\nu(n)$ impair), et la même propriété est héritée lorsque nous examinons les sous-ensembles de n qui sont divisibles par d tant que x/d n'est pas petit.

(2) La méthode du crible est, comme nous l'avons vu dans la section 15, assez tolérante envers les termes de reste R_d plus grossiers dans l'expression de N_d.

Il découle de ceci bien sûr qu'un crible en soi ne contient aucune caractéristique capable de faire une distinction entre les deux classes d'entiers. Il s'ensuit que si nous n'avions pas fait la distinction en sélectionnant nos ensembles pondérés avec un biais intégré vers $\nu(n)$ impair ou pair, le résultat de l'application du crible aurait été à peu près également divisé entre la contribution des deux classes d'entiers [9].

J'ai rencontré ce phénomène pour la première fois en 1946, alors que j'explorais la méthode Λ^2, d'abord en relation avec les bornes supérieures, comme par exemple dans le résultat

$$\pi(x+y) - \pi(y) \leq \frac{2y}{\log y} + \mathrm{O}\left(\frac{y}{\log^2 y}\right), \tag{18.1}$$

que j'ai obtenu très tôt, puis en essayant de diverses manières de l'adapter afin de me donner des bornes inférieures. Je n'ai pas prêté beaucoup d'attention à l'époque au facteur 2 dans (18.1) (si ce n'est pour noter qu'il s'agissait d'une amélioration par rapport à ce que d'autres avaient obtenu), mais ce qui a attiré mon attention et a changé l'orientation de mon intérêt pour le crible alors que j'essayais de le comprendre, c'est ce qui suit : à l'automne 1946, je considérais les deux expressions

$$Q_1(\lambda) = \sum_{x \leq n \leq (1+\epsilon)x} \left(\sum_{d|n} \lambda_d\right)^2,$$

et

$$Q_2(\lambda) = \sum_{x \leq n \leq (1+\epsilon)x} \tau(n) \left(\sum_{d|n} \lambda_d\right)^2,$$

où c est une constante positive et $\tau(n)$ la fonction diviseur. Comme d'habitude, j'ai posé $\lambda_1 = 1$ et j'ai laissé les autres λ être disposés de la manière la plus favorable. Mon objectif était de voir à quel point je pouvais réduire le rapport $Q_2(\lambda)/Q_1(\lambda)$.

8. Référence : A. Selberg, Lectures on Sieves, dans Collected Papers, vol. II, Springer-Verlag, Berlin, 1991, section 18 "A historical digression, the parity principle and a further example", p. 202-205.

9. Comme on peut facilement s'en convaincre, il n'en va pas de même si l'on divise les entiers en classes distinctes selon le résidu de $\nu(n) \pmod q$ pour $q > 2$.

Dans $Q_2(\lambda)$, le terme principal est essentiellement (j'omets certaines fonctions additives qui sont insignifiantes par rapport au logarithme),

$$Q_2'(\lambda) = cx \sum_{d,d'} \tau\left(\frac{dd'}{\kappa}\right) \frac{\kappa}{dd'} \lambda_d \lambda_{d'} \log \frac{x}{dd'} ,$$

où $\kappa = (d, d')$. Ceci ne peut pas être entièrement mis sous forme diagonale par notre transformation habituelle, mais si nous prenons simplement $\log x$ au lieu de $\log \frac{x\kappa}{dd'}$, il est facilement diagonalisable et minimisé. Si nous exigeons $\lambda_d = 0$ pour $d > \sqrt{x}$, par exemple, afin de maintenir les termes de reste suffisamment petits, nous obtenons

$$\lambda_d \approx \mu(d) \left(1 - 2 \frac{\log d}{\log x}\right)^2$$

pour $1 \le d \le \sqrt{x}$. En insérant ces valeurs dans $Q_2(\lambda)$ et $Q(\lambda_1)$. Je pourrais montrer qu'avec ce choix

$$\frac{Q_2(\lambda)}{Q_1(\lambda)} = 4 + \mathrm{O}\left(\frac{1}{\log x}\right). \tag{18.2}$$

Ceci montre bien sûr qu'il existe un nombre significatif de n dans l'intervalle avec $\tau(n) \le 4$, c'est-à-dire des nombres premiers ou des produits de deux nombres premiers, puisque les carrés des nombres premiers (avec $\tau(n) = 3$) sont trop peu nombreux pour contribuer.

Puisque le rapport (18.2) a été obtenu non pas en essayant de minimiser Q_2/Q_1, mais plutôt en minimisant simplement la partie la plus significative de Q_2, j'étais assez sûr que le minimum réel s'avérerait être < 4, et donc la présence de nombres premiers dans l'intervalle $x \le n \le (1 + c)x$ pour tout $c > 0$ fixé et pour suffisamment grand pourrait être établie. Cela me semblait un résultat intéressant, s'il pouvait être obtenu par des moyens élémentaires, alors j'ai consacré beaucoup de temps à essayer d'obtenir le minimum réel du rapport. Finalement, et à ma grande surprise, j'ai constaté que je ne pouvais pas amener le rapport en dessous de 4.

J'ai ensuite commencé à analyser les contributions des différentes classes d'entiers : nombres premiers, produits de deux nombres premiers, de trois nombres premiers, etc., aux expressions Q_1 et Q_2, et j'ai remarqué que mon choix initial de λ_d éliminait essentiellement les contributions des n avec $\nu(n)$ pair, à l'exception de ceux avec $\nu(n) = 2$ ($\nu(n) = 0$ n'apparaît pas dans l'intervalle considéré), à la fois à Q_2 et à Q_1. En même temps, j'ai constaté que Q_2 et Q_1 étaient assez équitablement répartis entre les contributions provenant des n avec $\nu(n)$ pair et celles provenant des n avec $\nu(n)$ impair. Ainsi, le rapport devait clairement être d'environ 4. De plus, si les λ étaient modifiés de manière à rendre la contribution des n avec $\nu(n) > 2$ et pair non négligeable, le rapport augmenterait, de sorte que le nombre 4 dans (18.2) devrait être remplacé par un nombre plus grand. Je comprenais maintenant aussi pourquoi la constante 2 apparaissait dans (18.1), et qu'elle ne pouvait pas être remplacée par une constante plus petite.

C'est ce qui a suscité mon intérêt pour l'étude des limites des méthodes de crible en général. Tout ce travail a été motivé et guidé par ce principe auquel j'ai finalement décidé de donner un nom (au milieu des années soixante-dix, lorsque j'ai donné des conférences sur ce sujet), je l'ai appelé “le

principe de parité".

Ce principe peut être formulé comme suit :

Les ensembles d'entiers ont tendance à être très uniformément répartis par rapport à la parité de leur nombre de facteurs premiers, à moins qu'ils n'aient été particulièrement produits, construits ou sélectionnés d'une manière qui présente un biais intégré. Il en va de même pour les ensembles de r-uplets $(n_1, ..., n_r)$ lorsque nous les divisons en 2^r classes selon les parités de $\nu(n_1), \ldots, \nu(n_r)$, s'il n'existe en outre aucun lien entre les parités des membres des r-uplets.

Ce principe ne peut bien sûr pas être "prouvé" comme étant valide en général. Mais il fournit une bonne ligne directrice pour évaluer ce qu'une approche particulière via une méthode de crible peut donner, ainsi que pour construire des modèles qui montrent que certains résultats ne peuvent pas être atteints par l'application directe d'un crible, qu'il s'agisse du criblage classique ou du criblage avec pondération.

Une fois ces limitations comprises, il est également possible de les exploiter. C'est ma compréhension, encore assez vague, du principe de parité qui m'a donné l'idée de concevoir un crible "local" [10] qui, entre 1 et x, ne compterait que les nombres ayant un ou deux facteurs premiers et éliminerait les autres. Cela a ensuite conduit à la démonstration élémentaire du théorème de Dirichlet sur les progressions arithmétiques, ainsi qu'à la démonstration élémentaire du théorème des nombres premiers. Bien que j'aie expérimenté avec plusieurs cribles locaux de ce type (qui conduisent tous à des résultats asymptotiques lorsqu'ils sont appliqués à l'intervalle $(1, x)$ ou $(x, 2x)$ par exemple), je n'ai publié que celui que je considérais comme le plus simple. Plus tard, l'idée a été développée beaucoup plus loin, d'abord par Diamond en lien avec l'amélioration du terme de reste dans la démonstration élémentaire du théorème des nombres premiers, puis de manière beaucoup plus générale par Bombieri, qui, dans ce qu'il a appelé le crible asymptotique (car il conduit à des formules asymptotiques), a transformé le crible local en un outil très polyvalent et puissant.

Nous n'aborderons pas les cribles locaux dans cet exposé. Revenant au sujet des dernières sections, nous construirons un modèle conçu pour illustrer les limitations d'un problème de criblage avec pondération. Le problème est le suivant :

Supposons que nous ayons donné un ensemble d'entiers positifs n_i, avec des poids associés w_i tels que tout $n_i \leq x$ et tels que si nous posons

$$y = \sum_i w_i$$

nous ayons

$$\sum_{d|n_i} w_i = \frac{u(d)}{d} y + R_d \ ,$$

10. Par crible local, nous entendons un système Λ qui fonctionne comme un crible uniquement sur des ensembles de nombres dont les valeurs absolues sont inférieures à une certaine limite spécifique.

où les $u(d)$ correspondent à une densité de criblage 1 au sens fort, disons

$$\sum_{p\leq x^{\alpha}} \frac{u(p)}{p} \log p = \alpha \log x + \mathrm{O}(1),$$

et les R_d satisfont des conditions telles que le criblage peut être effectué avec un crible $\Lambda^-[P(x^{\alpha}), \sigma, z]$ du moment que z est légèrement inférieur à $\sqrt{x}$. Est-il alors possible de choisir les poids σ et Λ^- de manière à ce que nous puissions prouver qu'existent des n_i qui ne contiennent pas plus de 2 facteurs premiers ?

Ceci se rapporte à plusieurs problèmes classiques, notamment au problème de montrer qu'il existe des nombres premiers entre x et $x + \sqrt{x}$ pour x grand, ou qu'un polynôme irréductible du second degré comme $n^2 + 1$ représente une infinité de nombres premiers. Ici, on essaie d'attaquer le problème en montrant que l'énoncé est vrai si l'on remplace "premier" par "nombre avec au plus r facteurs premiers" et ensuite on essaie de le prouver avec un r aussi petit que possible.

Le problème des nombres premiers jumeaux et le problème de Goldbach conduisent également à ce type de question, si l'on formule par exemple le problème des nombres premiers jumeaux comme la question de savoir si l'ensemble des $p + 2$, avec $x/2 \leq p < x$ pour x grand, contient toujours des nombres premiers.

Le fait que l'on puisse répondre par l'affirmative à ces deux premiers problèmes, avec $r = 3$, a été réalisé assez tôt [11]. En revanche, pour les deux derniers problèmes cités, on ne pouvait pas les aborder de cette manière sans supposer l'hypothèse générale de Riemann pour la fonction zêta et les fonctions L de Dirichlet, qui étaient nécessaires pour montrer que les R_d ne se comportaient pas trop mal. Ce n'est qu'après le théorème de Bombieri [12] en 1965 que l'on a pu obtenir $r = 3$ sans aucune hypothèse.

Le modèle que nous allons construire sera spécialement conçu pour modéliser le problème des nombres premiers jumeaux, mais il pourrait tout aussi bien être conçu pour imiter les conditions de N_d et R_d dans les autres problèmes mentionnés.

Le résultat de Bombieri donne ce qui suit pour le problème des nombres premiers jumeaux :

Si nous considérons l'ensemble des nombres

$$p + 2$$

où p arcourt les nombres premiers $\leq x$ et les pondère avec le poids $\log p$, et posons, pour d impair,

$$N_d = \sum_{\substack{d|p+2 \\ p\leq x}} \log p = \frac{x}{\varphi(d)} + R_d, \tag{18.3}$$

11. Le résultat pour n^2+1 avec $r = 3$ est mentionné pour la première fois dans une note de bas de page de (Selberg 2, p. 17] $\stackrel{?}{=}$ Selberg A., *On elementary methods in prime number theory.*, C. R. 11 Skand. Math. Kong. Trondheim, 1949, p. 13-22.

12. [Bombieri 1] = Bombieri,E., *On the large sieve*, Mathematika, 12 (1965), p. 201-225.

nous avons

$$\sum_{d\leq x} |R_d| = \mathrm{O}(x^{1/2} z\ (\log x)^5) \tag{18.4}$$

pour $x^{1/2}(\log x)^{-A} \leq z < x^{1/2}$, où $A > 0$ est un nombre fixé quelconque.

Dans la construction de notre modèle, nous supposerons par souci de simplicité l'hypothèse de Riemann pour la fonction zêta. Il est bien connu que alors

$$\sum_{n\leq x} \lambda(n) = \mathrm{O}(x^{1/2+\epsilon}). \tag{18.5}$$

pour tout $\epsilon > 0$ fixé. La même estimation est clairement valable si nous ne sommons que sur les nombres impairs n.

Nous définissons maintenant une fonction totalement multiplicative $g(n)$ définie comme suit, $g(2) = 0$ et $g(p) = p/(p-1)$ pour $p > 2$. Nous avons alors pour n impair, que

$$g(n) = \sum_{\delta|n} g'(\delta),$$

où g' est une fonction multiplicative avec $g'(p^r) = p^{r-1}/(p-1)^r$ pour $r > 0, p > 2$. Nous pouvons alors facilement montrer

$$\sum_{n\leq x} g(n) = cx + \mathrm{O}(x^{1/2}),$$

où

$$c = \frac{1}{2} \prod_{p>2} \left(1 + \frac{1}{p(p-2)}\right),$$

et

$$\sum_{n\leq x} \lambda(n) g(n) = \mathrm{O}(x^{1/2}).$$

De cela, nous déduisons, pour d impair et sans facteur carré,

$$\sum_{\substack{d|n \\ n\leq x}} (1+\lambda(n)) g(n) = \frac{cx}{\varphi(d)} + \mathrm{O}\left(\left(\frac{x}{d}\right)^{1/2+\epsilon} \frac{d}{\varphi(d)}\right) \tag{18.6}$$

Nous définissons maintenant un ensemble de nombres n comme suit : $n = mp$, où $1 < m \leq \sqrt{x/2}$ et $\sqrt{x} < p \leq \sqrt{2x}$, nous attribuons à ces nombres n des poids

$$w_n = (1+\lambda(m)) g(m) \rho_p \tag{18.7}$$

où les ρ_p pour les nombres premiers p dans l'intervalle $\sqrt{x} < p < \sqrt{2x}$ sont > 0 et tels que

$$\sum_{\sqrt{x}<p\leq\sqrt{2x}} \rho_p = \frac{1}{c}\sqrt{2x}.$$

Nous avons alors pour $d \leq \sqrt{x}$,

$$N_d = \sum_{d|n} w_n = \frac{x}{\varphi(d)} + R_d \tag{18.8}$$

avec

$$R_d = \mathrm{O}\left(\frac{x^{3/4+\epsilon} d^{1/2-\epsilon}}{\varphi(d)}\right) \tag{18.9}$$

de sorte que pour $z \leq \sqrt{x}$

$$\sum_{d \leq z} = \mathrm{O}(x^{3/4+\epsilon} z^{1/2-\epsilon}). \tag{18.10}$$

Bien que cela ne soit pas tout à fait identique à la forme de (18.4), nous voyons que pour, disons, z de la forme $x^{1/2}(\log x)^{-A}$, (18.4) a comme terme O(−)

$$\mathrm{O}\left(\frac{x}{(\log x)^{A-5}}\right) ,$$

tandis que (18.10) donne

$$\mathrm{O}\left(\frac{x}{(\log x)^{(1/2-\epsilon)A}}\right) ,$$

Puisque $u(p)$ =p/(p-1)*pour*p > 2*correspond*àk = 1*ete*$_u(\mathcal{P}(x^\alpha)) \sim c'/(\alpha \log x)$, on constate qu'on peut en fait pousser le criblage légèrement plus loin avec la condition (18.10) qu'avec (18.4), ou autrement dit, on peut appliquer des cribles $\Lambda^-[\mathcal{P}(x^\alpha), \sigma, z|$ avec un $z = x^{1/2}(\log x)^{-A}$ avec un A légèrement plus petit, et on devrait donc pouvoir faire au moins aussi bien avec l'ensemble pondéré modèle qu'avec les $p + 2$ avec le poids $\log p$. Mais l'ensemble modèle ne contient tout simplement aucun nombre avec moins de 3 facteurs premiers. *Il est donc impossible, par application d'un crible pondéré, de prouver qu'existent $p + 2$ nombres avec moins de 3 facteurs premiers, en se basant uniquement sur les informations contenues dans (18.3) et (18.4).*

Il en va de même pour les autres problèmes mentionnés ci-dessus ; nous aurions pu adapter notre modèle pour en imiter un. Il n'en reste pas moins que pour tous ces problèmes, une réponse affirmative a été apportée. Tout d'abord par Jing-Run Chen, qui a prouvé qu'il existe une infinité de p pour lesquels $p + 2$ n'a pas plus de deux facteurs premiers, et a en même temps prouvé le résultat correspondant lié au problème de Goldbach. Il a également résolu le problème consistant à établir qu'il existe toujours, pour de grandes valeurs de x, des nombres compris entre et $x + \sqrt{x}$ qui n'ont pas plus de deux facteurs premiers. Enfin, le problème consistant à montrer que $n^2 + 1$ représente une infinité de nombres ayant au plus deux facteurs premiers a été résolu par H. Iwaniec.

En général, les limitations que nous pouvons établir pour les méthodes de crible sont valides *seulement lorsque lorsqu'aucune information supplémentaire à celle donnée sur les N_d et $|R_d|$ n'est disponible.* Dans un problème "concret" spécifique comme ceux mentionnés ici, il est toujours possible d'introduire d'autres informations dans l'argument, ce qui peut permettre de dépasser ces limitations.