Article du blog de Terence Tao en 2007 à propos de l'obstruction dite "de la parité"

Question ouverte : Le problème de parité dans la théorie des cribles
5 juin, 2007, Tags : problème de parité, théorie du crible | par Terence Tao

Le problème de parité est un problème notoire dans la théorie du crible : cette théorie a été inventée afin de compter les nombres premiers de divers types (par exemple les nombres premiers jumeaux), mais malgré un superbe succès dans l'obtention de limites supérieures sur le nombre de tels modèles, cette théorie s'est avérée quelque peu décevante dans l'obtention de limites inférieures. [Les cribles peuvent également être utilisés pour étudier beaucoup d'autres choses que les nombres premiers, bien sûr, mais nous nous concentrerons uniquement sur les nombres premiers dans ce post.] Même la tâche de prouver le théorème d'Euclide - qu'il y a infiniment de nombres premiers - semble extrêmement difficile à faire par des techniques de théorie des cribles, à moins bien sûr d'injecter dans la théorie une estimation au moins aussi forte que le théorème d'Euclide (par exemple le théorème des nombres premiers (TNP)). La principale obstruction est le problème de parité : même en supposant des hypothèses aussi fortes que la conjecture d'Elliott-Halberstam (une sorte d'"hypothèse de Riemann super-généralisée" pour les cribles), la théorie des cribles est en grande partie (mais pas complètement) incapable de distinguer les nombres avec un nombre impair de facteurs premiers des nombres avec un nombre pair de facteurs premiers. Cette " barrière de parité " a été brisée pour certains modèles de nombres premiers en injectant des méthodes de théorie autres (que la théorie des cribles) puissantes dans le sujet, mais reste un formidable obstacle en général.

Je discuterai plus en détail du problème de parité plus loin dans ce post, mais je veux d'abord discuter de la façon dont les cribles fonctionnent [en partie sur d'excellentes notes de conférence inédites d'Iwaniec] ; les idées de base sont élémentaires et conceptuellement simples, mais il y a beaucoup de détails et de technicités impliqués dans l'exécution de ces idées, et que je vais essayer de supprimer pour en faciliter l'exposé.

Considérons une question de base dans la théorie des nombres premiers, à savoir comment compter le nombre de nombres premiers dans une plage donnée, disons entre N et $2N$ pour un grand nombre entier N. (Ce problème est plus ou moins équivalent à celui de compter les nombres premiers entre 1 et N, grâce à la décomposition dyadique, mais avec comme avantage de garder les grandeurs de tous les nombres comparables à N, nous pouvons simplifier certaines technicités (très mineures).) Bien sûr, nous savons que cette question particulière peut être réglée de manière assez satisfaisante (la réponse est $(1+o(1))\frac{N}{\log N}$) en utilisant des faits connus sur la fonction zêta de Riemann, mais faisons semblant pour l'instant que nous ne connaissons pas cette fonction. (Une fois que l'on passe à des questions additives légèrement plus compliquées sur les nombres premiers, telles que le comptage des nombres premiers jumeaux, la théorie de la fonction zêta et de ses parents devient beaucoup moins puissante, même en supposant des choses telles que l'hypothèse de Riemann ; le problème est que ces fonctions mesurent la structure multiplicative des nombres premiers plutôt que leur structure additive.)

Référence : https://terrytao.wordpress.com/2007/06/05/open-question-the-parity-problem-in-sieve-theory/.

L'ensemble des nombres premiers ne semble pas avoir assez de structure utilisable pour effectuer de tels comptages rapidement. Cependant, on peut compter d'autres ensembles de nombres entre N et $2N$ avec beaucoup plus de facilité. Par exemple, l'ensemble des entiers entre N et $2N$ peut être facilement compté avec une petite erreur :

$$|\{n \in [N, 2N] : n \text{ entier}\}| = N + \mathrm{O}(1);$$

le terme d'erreur $\mathrm{O}(1)$ dans ce cas est en fait seulement 1. De même, on peut compter, disons, le nombre de nombres impairs entre N et $2N$,

$$|\{n \in [N, 2N] : n \text{ odd}\}| = \frac{1}{2}N + \mathrm{O}(1),$$

simplement parce que l'ensemble des nombres impairs a de la densité $\frac{1}{2}$ et est périodique de la période 2. Le terme d'erreur $\mathrm{O}(1)$ dépend maintenant de la parité de N. Plus généralement, nous pouvons compter n'importe quelle classe de résidus donnée sur $[N, 2N]$ avec une précision raisonnable :

$$|\{n \in [N, 2N] : n \equiv a \pmod q\}| = \frac{1}{q}N + \mathrm{O}(1),$$

où le terme d'erreur est maintenant plus compliqué, et dépend du reste de N modulo q. Cette estimation est assez bonne tant que q est petit par rapport à N, mais lorsque q est très grand, le terme d'erreur $\mathrm{O}(1)$ peut commencer à submerger le terme principal (surtout si le terme principal va apparaître dans une somme délicate avec beaucoup d'annulation). D'une manière générale, toute somme impliquant le terme principal N/q sera relativement facile à manipuler (car elle est essentiellement multiplicative en q, et donc favorable à toutes les méthodes de théorie des nombres multiplicatifs, en particulier les produits eulériens et les fonctions zêta) ; c'est le terme d'erreur $\mathrm{O}(1)$ qui cause toute la difficulté.

Une fois que nous avons compris comment compter ces ensembles de base, nous pouvons également compter certaines combinaisons de ces ensembles, tant que ces combinaisons sont assez simples. Par exemple, supposons que nous voulons compter

$$|\{n \in [N, 2N] : n \text{ premier a } 2, 3\}|. \tag{1}$$

Nous savons que le nombre total d'entiers dans l'intervalle $[N, 2N]$ est $N + \mathrm{O}(1)$. Au sein de cet ensemble, nous savons que $\frac{1}{2}N + \mathrm{O}(1)$ nombres ne sont pas premiers avec 2 (c'est-à-dire qu'ils sont divisibles par 2) et que $\frac{1}{3}N + \mathrm{O}(1)$ ne sont pas premiers avec 3. Si nous soustrayons ces deux sous-ensembles de l'ensemble initial, il reste $\frac{1}{6}N + \mathrm{O}(1)$. Toutefois, les nombres divisibles à la fois par 2 et par 3 (c'est-à-dire divisibles par 6) ont été soustraits deux fois ; il faut donc les réintégrer, ce qui ajoute $\frac{1}{6}N + \mathrm{O}(1)$ et aboutit à un décompte final de $\frac{1}{3}N + \mathrm{O}(1)$ pour la quantité (1) ; il s'agit bien entendu d'une simple application du principe d'inclusion-exclusion. Une autre façon d'estimer (1) consiste à utiliser le théorème des restes chinois pour réécrire (1) sous la forme

$$|\{n \in [N, 2N] : n \equiv 1, 5 \pmod 6\}|$$

et à s'appuyer sur notre capacité à compter les classes de restes modulo 6 pour obtenir le même résultat de $\frac{1}{3}N + \mathrm{O}(1)$ (bien que la borne précise du terme d'erreur diffère légèrement). Pour de

très petits modules tels que 2 et 3, le théorème des restes chinois est très efficace, mais il manque de souplesse ; pour des modules plus élevés (par exemple, bien supérieurs à $\log N$), il s'avère que le principe d'inclusion-exclusion, plus flexible, donne de bien meilleurs résultats (moyennant quelques astuces pour en optimiser l'efficacité).

Nous pouvons bien sûr poursuivre l'exemple (1) en comptant les nombres de l'intervalle $[N, 2N]$ qui sont premiers avec 2, 3, 5, 7, etc. - ce qui, grâce au crible d'Ératosthène, finira par nous donner le nombre de nombres premiers dans $[N, 2N]$ - mais prenons un instant pour considérer la situation dans son ensemble. Nous avons vu que certains ensembles dans l'intervalle $[N, 2N]$ sont relativement faciles à dénombrer avec précision (par exemple, les classes de résidus modulo un petit entier), tandis que d'autres ne le sont pas (comme les nombres premiers ou les nombres premiers jumeaux). Quelle est la caractéristique déterminante des premiers ? Une réponse plausible est que ces ensembles faciles à dénombrer présentent une faible complexité, mais ce terme reste assez vague. Je propose plutôt de considérer que les ensembles (ou, plus généralement, les fonctions de poids - voir ci-dessous) sont faciles à dénombrer (ou du moins à estimer) lorsqu'ils sont "réguliers" (*smooth*), au sens d'une notion que je préciserai sous peu. Cette terminologie est empruntée à l'analyse harmonique plutôt qu'à la théorie des nombres (bien que cette dernière connaisse le concept apparenté de "nombre régulier" (ou *smooth number*) ; je vais donc faire une brève digression sur la notion de régularité, car il me semble qu'elle sous-tend implicitement la stratégie fondamentale de la théorie du crible. Au lieu de parler du problème de comptage (environ) d'un ensemble donné dans $[N, 2N]$, considérons plutôt le problème analogue de (environ) calculer la zone d'une région E donnée (par exemple une ellipse solide) dans le carré de l'unité $[0, 1]^2$. Comme on nous l'enseigne au lycée, une façon de le faire est de subdiviser la région E de l'unité en carrés plus petits, par exemple des carrés de longueur 10^{-n} pour certains n, et de compter combien de ces petits carrés se trouvent complètement ou partiellement dans l'ensemble E, et de multiplier par la zone de chaque carré ; c'est bien sûr le prélude à l'intégrale de Riemann. Il fonctionne bien tant que l'ensemble E est " lisse " en ce sens que la plupart des petits carrés sont soit complètement à l'intérieur, soit complètement à l'extérieur de l'ensemble E, avec peu de cas sur la frontière ; cette notion de douceur peut également être considérée comme une version quantitative de la mesurabilité de Lebesgue. Une autre façon de dire cela est que si l'on veut déterminer si un point donné (x, y) se trouve dans E, il suffit généralement de calculer x et y aux n premiers chiffres significatifs dans l'expansion décimale.

Revenons au dénombrement d'ensembles dans l'intervalle $[N, 2N]$. On peut également définir ici la notion d'"ensemble lisse" en utilisant, là encore, les chiffres les plus significatifs des nombres n de cet intervalle ; par exemple, l'ensemble $[1.1N, 1.2N]$ serait considéré comme assez lisse, car il serait aisé de déterminer si n appartient ou non à cet ensemble en examinant simplement les deux ou trois premiers chiffres significatifs. Toutefois, avec cette conception "euclidienne" ou "archimédienne" de la lissité, des ensembles tels que celui des nombres premiers ou celui des nombres impairs ne sont assurément pas lisses. La situation s'améliore considérablement si l'on change de métrique ou, plus informellement, si l'on redéfinit ce qu'est le "chiffre le plus significatif". Par exemple, si l'on considère le dernier chiffre du développement décimal d'un nombre n (c'est-à-dire la valeur de $n \pmod{10}$) comme étant le plus significatif - ou, plus précisément, si l'on utilise la métrique 10-adique au lieu de la métrique euclidienne, plongeant ainsi les entiers dans $\mathbb{Z}_{10}$ plutôt que dans $\mathbb{R}$ - alors les nombres impairs deviennent tout à fait lisses (le chiffre le plus significatif détermine entièrement l'appartenance à cet ensemble). Les nombres premiers de l'intervalle $[N, 2N]$ ne sont

pas parfaitement lisses, mais ils présentent une certaine lissité partielle ; en effet, si le chiffre le plus significatif est 0, 2, 4, 5, 6 ou 8, l'appartenance à l'ensemble est entièrement déterminée, alors que si ce chiffre est 1, 3, 7 ou 9, on ne dispose que d'une information partielle quant à l'appartenance à l'ensemble.

Cela dit, la métrique 10-adique ne permet pas de caractériser de manière pleinement satisfaisante le concept insaisissable de "lissité" en théorie des nombres. Par exemple, l'ensemble des multiples de 3 devrait être lisse, ce qui n'est pas le cas avec la métrique 10-adique (il faut en réalité connaître tous les chiffres pour savoir avec certitude si un nombre est un multiple de 3 !). Par ailleurs, cette approche soulève une autre difficulté : l'ensemble $[N/2, N]$ lui-même cesse alors d'être lisse. On peut remédier à cela en travaillant non pas uniquement avec la métrique euclidienne ou une unique métrique n-adique, mais avec le produit de toutes les métriques n-adiques et de la métrique euclidienne simultanément. En fait, grâce au théorème des restes chinois, il suffit de considérer le produit des métriques p-adiques (pour les nombres premiers p) et de la métrique euclidienne, plongeant ainsi les entiers dans l'anneau des adèles $\mathbb{R} \times \prod_p \mathbb{Z}_p$. Pour une raison étrange, cet anneau d'adèles n'est pas explicitement utilisé dans la plupart des exposés sur la théorie du crible, malgré sa pertinence évidente (et malgré l'utilité amplement démontrée de cet anneau en théorie algébrique des nombres ou en théorie des fonctions L, comme l'illustre par exemple la thèse de Tate). Quoi qu'il en soit, nous n'utilisons la notion de "lissité" (*smoothness*) que dans un sens très informel ; nous n'aurons donc pas besoin ici de tout le formalisme des adèles. Disons simplement qu'un ensemble d'entiers dans $[N, 2N]$ est "lisse" si l'appartenance à cet ensemble est largement déterminée par ses chiffres les plus significatifs au sens euclidien, ainsi qu'au sens p-adique pour les petits p ; en gros, cela signifie que cet ensemble est approximativement l'image réciproque d'un ensemble de "faible complexité" dans l'anneau des adèles - un ensemble pouvant être construit efficacement à partir de quelques ensembles élémentaires engendrant la topologie et la tribu de cet anneau. (En fait, dans de nombreuses applications de la théorie du crible, il suffit de considérer des modules q sans facteur carré ; on peut alors remplacer les anneaux p-adiques $\mathbb{Z}_p$ par les groupes cycliques $\mathbb{Z}/p\mathbb{Z}$. Ainsi, ce sont désormais les résidus modulo p pour les petits p, combinés aux chiffres euclidiens les plus significatifs, qui déterminent la nature des ensembles lisses ; l'anneau des adèles se trouve alors remplacé par le produit $\mathbb{R} \times \prod_p (\mathbb{Z}/p\mathbb{Z})$.)

Revenons maintenant à la théorie des cribles, et à la tâche de compter les ensembles "rugueux" tels que les nombres premiers dans $[N, 2N]$. Puisque nous savons comment compter avec précision les ensembles "lisses" tels $\{n \in [N, 2N] : n \equiv a \pmod q\}$ qu'avec q petit, on peut essayer de décrire l'ensemble rugueux des nombres premiers comme une sorte de combinaison d'ensembles lisses. L'implémentation la plus directe de cette idée est le crible d'Ératosthène ; si l'on essaie alors de calculer le nombre de nombres premiers en utilisant le principe d'inclusion-exclusion, on obtient le crible de Legendre ; nous avons implicitement utilisé cette idée précédemment lors du comptage de la quantité (1). Cependant, le nombre de termes dans la formule d'inclusion-exclusion est très important (2^k) ; si l'on exécute le crible de l'Ératosthène pour k étapes (c'est-à-dire en criblant des multiples des k premiers nombres premiers), il existe de façon essentielle des termes dans la formule d'inclusion-exclusion, conduisant à un terme d'erreur qui dans le pire des cas pourrait être de taille $O(2^k)$. Un problème connexe est que le module q dans de nombreux termes dans le crible de Legendre devient assez grand - aussi grand que le produit des k premiers nombres premiers (qui s'avère être à peu près de taille e^k). Puisque l'ensemble que l'on essaie de compter n'est que de taille

N, nous voyons donc que le crible de Legendre devient inutile juste après les $\log N$ étapes au plus plus du crible d'Ératosthène, ce qui est bien à court de ce dont on a besoin pour compter avec précision les nombres premiers (ce qui nécessite que l'on utilise $N^{1/2}/\log N$ ou avoisinant des étapes). Plus généralement, les cribles "exacts" tels que le crible de Legendre sont utiles pour toute situation impliquant logarithmiquement seulement un petit nombre de modules, mais ne conviennent pas au criblage avec un nombre beaucoup plus grand de modules.

On peut décrire les débuts de la théorie du crible comme un effort concerté pour remédier aux défauts du crible de Legendre. La première idée maîtresse consiste ici à ne pas chercher à calculer exactement la taille de l'ensemble "brut" - car cela s'avère trop "coûteux" en termes de nombre d'ensembles "lisses" nécessaires pour le décrire complètement - mais plutôt à se contenter de bornes supérieures ou inférieures pour la taille de cet ensemble, en utilisant moins d'ensembles lisses. Il existe ainsi un compromis entre la précision avec laquelle les bornes approchent l'ensemble initial et la facilité avec laquelle on peut calculer ces bornes ; en choisissant judicieusement divers paramètres, on peut optimiser ce compromis et obtenir une borne finale qui soit non triviale, sans pour autant être parfaitement exacte. Par exemple, si l'on utilise le crible de Legendre pour tenter de compter les nombres premiers compris entre N et $2N$, on peut plutôt s'en servir pour dénombrer l'ensemble - bien plus vaste - des nombres compris entre N et $2N$ qui sont premiers avec les k premiers nombres premiers, obtenant ainsi une borne supérieure pour le nombre de nombres premiers dans cet intervalle. Il s'avère que la valeur optimale de k est alors de l'ordre de $\log N$ (au-delà, les termes d'erreur du crible de Legendre deviennent incontrôlables), ce qui fournit une borne supérieure en $O(N/\log\log N)$ pour le nombre de nombres premiers entre N et $2N$; ce résultat est certes assez éloigné de la réalité (qui est $\sim N/\log N$), mais il demeure non trivial.

Dans le même ordre d'idées, on peut travailler avec diverses versions tronquées ou approchées de la formule du crible (ou principe d'inclusion-exclusion) impliquant moins de termes. Par exemple, pour estimer le cardinal $|\bigcup_{j=1}^k A_j|$ de la réunion de k ensembles, on peut remplacer la formule du crible par inclusion-exclusion par

$$|\bigcup_{j=1}^k A_j| = \sum_{j=1}^k |A_j| - \sum_{1\leq j_1<j_2\leq k} |A_{j_1}\cap A_{j_2}| + \sum_{1\leq j_1<j_2<j_3\leq k} |A_{j_1}\cap A_{j_2}\cap A_{j_3}| \dots \quad (2)$$

par la borne supérieure évidente

$$|\bigcup_{j=1}^k A_j| \leq \sum_{j=1}^k |A_j|$$

(aussi appelée inégalité de Boole ou borne de l'union), ou par la borne inférieure, légèrement moins évidente,

$$|\bigcup_{j=1}^k A_j| \geq \sum_{j=1}^k |A_j| - \sum_{1\leq j_1<j_2\leq k} |A_{j_1}\cap A_{j_2}|.$$

Plus généralement, si l'on considère les n premiers termes du membre de droite de (2), on obtient une borne supérieure du membre de gauche pour n impair et une borne inférieure pour n pair. Ces inégalités, connues sous le nom d'inégalités de Bonferroni, constituent un exercice de démonstration

intéressant : elles découlent de l'observation que, dans l'identité binomiale

$$0 = (1-1)^m = \binom{m}{0} - \binom{m}{1} + \binom{m}{2} - \binom{m}{3} + \ldots + (-1)^m \binom{m}{m}$$

pour tout $m \geq 1$, les sommes partielles du membre de droite alternent entre des valeurs positives ou nulles et des valeurs négatives ou nulles. En intégrant ces inégalités au crible de Legendre et en optimisant le paramètre, on peut améliorer la borne supérieure du nombre de nombres premiers dans l'intervalle $[N, 2N]$ pour obtenir $O(N \log\log N / \log N)$, ce qui est bien plus proche de la réalité. Malheureusement, cette méthode ne fournit aucune borne inférieure autre que la borne triviale 0 ; soit le terme principal est négatif, soit le terme d'erreur l'emporte sur le terme principal. Un raisonnement analogue a été utilisé par Brun pour démontrer que le nombre de nombres premiers jumeaux dans $[N, 2N]$ est en $O(N(\log\log N / \log N)^2)$ (là encore, la valeur conjecturée est $\sim N / \log^2 N$), ce qui a conduit à son célèbre théorème selon lequel la somme des inverses des nombres premiers jumeaux converge.

L'extension complète inclusion-exclusion est une somme par 2^k rapport aux termes, que l'on peut voir comme des chaînes binaires de 0 et 1 de longueur k. Dans les inégalités de Bonferroni, on ne compte qu'une plus petite collection de chaînes de bits, à savoir la boule de Hamming de chaînes qui n'impliquent que n ou moins 1. Il existe d'autres collections de chaînes que l'on peut utiliser qui mènent à des bornes supérieures ou inférieures ; on peut imaginer révéler une telle chaîne un chiffre à la fois, puis décider de garder ou de jeter cette chaîne une fois qu'une règle de seuil est atteinte. Il existe différentes façons de sélectionner ces règles de seuillage, conduisant à la famille des cribles combinatoires. Une telle règle particulièrement efficace est similaire à celle donnée par les inégalités de Bonferroni, mais au lieu d'utiliser le nombre de 1 dans une chaîne pour déterminer l'appartenance à la sommation, on utilise un nombre pondéré de 1 (en donnant aux grands nombres plus élevés que les petits nombres premiers, car ils ont tendance à augmenter le module trop rapidement et doivent donc être retirés de la somme plus tôt que les petites nombres premiers). Cela conduit au crible bêta, qui donne par example l'ordre de grandeur correct du $O(N/\log N)O(N/\log^2 N)$ nombre de nombres de nombres premiers dans $[N, 2N]$ ou pour le nombre de nombres de nombres jumeaux dans $[N, 2N]$. Ce crible est également assez puissant pour donner des limites inférieures, mais seulement si l'on arrête le crible un peu tôt, élargissant ainsi l'ensemble des nombres premiers à un ensemble de presque premiers (nombres qui sont premiers à tous les nombres inférieurs à un certain seuil, et ont donc un nombre limité de facteurs premiers). Par exemple, ce crible peut montrer qu'il y a un nombre infini de jumeaux $(n, n+2)$, dont chacun a au plus neuf facteurs premiers (le neuf n'est pas optimal, mais obtenir de meilleurs résultats nécessite beaucoup plus de travail).

Il semble toutefois exister une limite à ce que peuvent accomplir les cribles purement combinatoires. Le problème provient du point de vue "binaire" de ces cribles : tout terme donné du développement d'inclusion-exclusion est soit inclus, soit exclu de la borne supérieure ou inférieure du crible, sans possibilité intermédiaire. Ceci conduit à l'idée principale suivante de la théorie moderne des cribles : travailler non pas avec les cardinalités des ensembles dans $[N, 2N]$, mais plutôt avec la notion plus flexible de sommes de fonctions de poids (fonctions à valeurs réelles sur $[N, 2N]$). Le point de départ est la formule évidente :

$$|A| = \sum_{n \in [N, 2N]} 1_A(n)$$

pour la cardinalité d'un ensemble A dans $[N, 2N]$, où 1_A est la fonction indicatrice de l'ensemble A. En appliquant ceci aux ensembles lisses tels que $\{n \in [N, 2N] : n \equiv a \pmod q\}$, on obtient :

$$\sum_{n \in [N,2N]} 1_{n \equiv a \pmod q}(n) = \frac{N}{q} + \mathrm{O}(1);$$

en particulier, en se spécialisant à la classe des résidus nuls $a \equiv 0$ (qui est la classe des résidus importante pour le dénombrement des nombres premiers), on a :

$$\sum_{n \in [N,2N]} 1_{d|n}(n) = \frac{N}{d} + \mathrm{O}(1)$$

pour tout d. Ainsi, si nous pouvons obtenir une borne supérieure ponctuelle sur 1_A par une somme de diviseurs (qui est un analogue en théorie des nombres d'une fonction lisse), alors

$$1_A(n) \leq \sum_d c_d \, 1_{d|n}(n) \tag{3}$$

pour tout n et certaines constantes réelles c_d (qui peuvent être positives ou négatives), alors, en sommant, nous obtenons la borne supérieure

$$|A| \leq N \sum_d \frac{c_d}{d} + \mathrm{O}(\sum_d |c_d|). \tag{4}$$

On peut également espérer obtenir des bornes inférieures pour $|A|$ grâce à une procédure similaire (bien qu'en pratique, l'obtention de bornes inférieures pour les nombres premiers se soit révélée beaucoup plus difficile en raison du problème de parité, que nous aborderons plus loin). Ces stratégies sont adaptées à la tâche de borner le nombre de nombres premiers dans l'intervalle $[N, 2N]$; si l'on souhaite réaliser une opération plus complexe, comme le décompte de nombres premiers jumeaux $(n, n+2)$, il faut soit faire intervenir davantage de classes de congruence (par exemple, la classe $a = -2$ jouera un rôle dans le problème des nombres premiers jumeaux), soit introduire des poids supplémentaires dans la sommation (par exemple, en affectant à chaque terme de la somme en n un facteur supplémentaire $\Lambda(n+2)$, où Λ désigne la fonction de von Mangoldt). Pour simplifier l'exposé, contentons-nous du problème plus élémentaire consistant à compter les nombres premiers.

Ces stratégies généralisent la stratégie de crible combinatoire, ce qui est un cas particulier dans lequel les constantes c_d sont limitées à $+1, 0$, ou -1. En pratique, la somme $\sum_d \frac{c_d}{d}$ en (4) est relativement facile à invoquer par des techniques de théorie des nombres multiplicatifs (les coefficients c_d, dans les applications, impliquent généralement la fonction Möbius (pas surprenante, puisqu'ils codent une sorte de principe d'inclusion-exclusion) et sont souvent liés aux coefficients d'une fonction zêta Hasse-Weil, car ils comptent essentiellement les solutions modulo d à certains ensembles d'équations algébriques), et la tâche principale est de s'assurer que pour ce faire, il faut essentiellement c_d concentrer les poids sur ceux qui sont relativement faibles par rapport à N, par exemple, ils peuvent être limités à une plage $d \leq R$ où le niveau $R = N^\theta$ de crible est d'une faible puissance de N. Ainsi, par exemple, en commençant par l'identité

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log(d), \tag{5}$$

qui correspond à l'identité de la fonction zeta

$$-\frac{\zeta'(s)}{\zeta(s)} = \zeta(s)\frac{d}{ds}\frac{1}{\zeta(s)},$$

où Λ est la fonction de von Mangoldt et μ est la fonction de Möbius, on obtient la borne supérieure

$$1_A(n) \leq -\sum_{d\leq 2N} \mu(d)\frac{\log d}{\log N} 1_{d|n}$$

où A désigne les nombres premiers de N à $2N$. Cela suffit déjà (avec l'asymptotique élémentaire $\sum_{d\leq 2N} \frac{\mu(d)}{d}\log d = \mathrm{O}(1)$) pour obtenir le faible théorème du nombre premier $|A| = \mathrm{O}(N/\log N)$, mais malheureusement cette méthode ne donne pas une borne inférieure non triviale pour $|A|$. Cependant, une variante de la méthode donne une bonne limite asymptotique pour P_2 les presque premiers - des produits d'au plus deux (grands) nombres premiers [par exemple des nombres premiers plus grands que N^ϵ pour certains valeurs fixes de $\epsilon > 0$]. En effet, si l'on introduit la seconde fonction de von Mangoldt

$$\Lambda_2(n) = \sum_{d|n} \mu(d)\log^2(\frac{n}{d}) = \Lambda(n)\log n + \sum_{d|n} \Lambda(d)\Lambda(\frac{n}{d}) \tag{6}$$

qui est principalement vérifié sur P_2 nombres presque premiers (en effet, $\Lambda_2(p) = \log^2 p$ et $\Lambda_2(pq) = 2\log p\log q$ pour des nombres premiers distincts p, q, et Λ_2 est presque nul sinon), et si on utilise la limite asymptotique élémentaire

$$\sum_{d\leq N} \frac{\mu(d)}{d}\log^2\frac{N}{d} = 2\log N + \mathrm{O}(1),$$

on obtient alors la formule de symétrie de Selberg

$$\sum_{n\leq N} \Lambda_2(N) = 2N\log N + \mathrm{O}(N).$$

Cette formule (avec le faible théorème P_2 de nombre premier mentionné précédemment) implique facilement un "théorème de nombre P_2 presque premier", à savoir que le nombre de nombres presque premiers inférieur à N est $(2+\mathrm{o}(1))\frac{N}{\log N}$. [Ce fait est beaucoup plus facile à prouver que le théorème des nombres premiers lui-même. En termes de fonctions zêta, la raison pour laquelle le théorème des nombres premiers est difficile est que le pôle simple de $\frac{\zeta'(s)}{\zeta(s)}s = 1$ pourrait être contrecarré par d'autres pôles simples sur la ligne $\mathrm{Re}(s) = 1$. D'autre part, le théorème P_2 au sujet des nombres presque premiers est beaucoup plus facile car l'effet du double pôle de $\frac{\zeta''(s)}{\zeta(s)}s = 1$ n'est pas contrecarré par les autres pôles sur la ligneRe(s)=1, qui sont au plus simples.]

Le théorème sur les nombres presque premiers de type P_2 établit le théorème des nombres premiers "à un facteur 2 près". Il est étonnamment difficile d'améliorer ce facteur 2 par des méthodes élémentaires ; toutefois, dès lors que l'on peut remplacer 2 par $2-\epsilon$ pour un certain $\epsilon > 0$ (fait essentiellement équivalent à l'absence de zéros de $\zeta(s)$ sur la droite $\mathrm{Re}(s) = 1$), on peut itérer

la formule de symétrie de Selberg (en s'appuyant sur le fait tautologique qu'un nombre presque premier de type P_2 est soit un nombre premier, soit le produit de deux nombres premiers) pour obtenir le théorème des nombres premiers ; c'est là, pour l'essentiel, la démonstration élémentaire de ce théorème due à Erdös et Selberg.

On peut obtenir d'autres bornes sur les diviseurs de la forme (3) grâce à diverses astuces, par exemple en modifiant les poids dans les formules (5) et (6) ci-dessus. Une borne supérieure étonnamment utile pour les nombres premiers compris entre N et $2N$ s'obtient par la simple observation suivante :

$$1_A(n) \leq \left(\sum_{d<N} \lambda_d 1_{d|n}(n) \right)^2$$

lorsque les λ_d sont des nombres réels arbitraires tels que $\lambda_1 = 1$, ce qui découle simplement du fait que le carré de tout nombre réel est positif ou nul. Cela conduit au crible de Selberg, qui suffit à de nombreuses applications ; il permet par exemple de démontrer l'inégalité de Brun-Titchmarsh, selon laquelle le nombre de nombres premiers compris entre N et $N + M$ est au plus $(2 + o(1))M/\log M$ - résultat qui, là encore, diffère d'un facteur 2 de la valeur exacte lorsque N et M sont d'ordres de grandeur comparables. Il existe également des bornes inférieures utiles pour la fonction indicatrice des nombres presque premiers définis par des sommes de diviseurs ; celles-ci peuvent servir, par exemple, à démontrer le théorème de Chen (affirmant qu'il existe une infinité de nombres premiers p tels que $p + 2$ soit un nombre presque premier de type P_2) ou le théorème selon lequel il existe une infinité de nombres presque premiers de type P_2 de la forme $n^2 + 1$.

En résumé, les méthodes de théorie des cribles peuvent fournir de bonnes limites supérieures, des limites inférieures et même des limites asymptotiques pour presque les nombres premiers, ce qui conduit à des limites supérieures pour les nombres premiers qui ont tendance à être éteintes par un facteur constant tel que 2. De manière plutôt frustrante, cependant, les méthodes de crible se sont avérées largement incapables de compter ou même de borner inférieurement le nombre des nombres premiers eux-mêmes, laissant ainsi la conjecture des nombres premiers jumeaux (ou la conjecture sur le fait qu'il existe une infinité de nombres premiers de la forme n^2+1) encore hors de portée. La raison de cela - le problème de parité - a d'abord été clarifiée par Selberg. Grosso modo, il affirme le :

> **Problème de la parité.** Si A est un ensemble dont les éléments sont tous des produits d'un nombre impair de nombres premiers (ou tous des produits d'un nombre pair de nombres premiers), alors (sans introduire d'ingrédients supplémentaires), la théorie du crible est incapable de fournir des minorations non triviales de la taille de A. De plus, toute majoration s'écartera nécessairement de la valeur réelle d'un facteur 2 ou plus.

Ainsi, on peut espérer compter les quasi-premiers de type P_2 (car ils peuvent avoir un nombre pair ou impair de facteurs), ou compter les nombres qui sont le produit de 6 ou 7 nombres premiers (ce qui est possible, par exemple, grâce au crible de Bombieri) ; en revanche, on ne peut espérer utiliser la théorie du crible classique pour compter simplement les nombres premiers ou les nombres pseudo-premiers (produit d'exactement deux nombres premiers).

Pour expliquer ce problème, nous introduisons la fonction de Liouville $\lambda(n)$ (étroitement liée à la fonction de Möbius), qui vaut $+1$ lorsque n est le produit d'un nombre pair de nombres premiers et -1 dans le cas contraire. Le problème de parité se pose donc dès lors que λ est identiquement égale à $+1$ ou à -1 sur l'ensemble A considéré.

La fonction de Liouville oscille de façon assez aléatoire entre $+1$ et -1. En effet, le théorème des nombres premiers s'avère équivalent à l'affirmation que λ est asymptotiquement nulle en moyenne,

$$\sum_{n \leq N} \lambda(n) = \mathrm{o}(N)$$

(un fait d'abord observé par Landau), et si l'hypothèse de Riemann est vraie alors on a une estimée bien meilleure

$$\sum_{n \leq N} \lambda(n) = O_\epsilon(N^{1/2+\epsilon}) \text{ pour tout } \epsilon > 0.$$

En supposant l'hypothèse de Riemann, on a une assertion similaire pour les classes de résidus modulaires :

$$\sum_{n \leq N} 1_{n \equiv a \pmod q} \lambda(n) = O_\epsilon(N^{1/2+\epsilon}) \text{ pour tout } \epsilon > 0.$$

Ce que cela signifie essentiellement, c'est que la fonction de Liouville est essentiellement orthogonale à tous les ensembles lisses, ou toutes les fonctions lisses. Puisque la théorie des cribles tente de tout estimer en termes d'ensembles et de fonctions lisses, elle ne peut donc pas éliminer une ambiguïté inhérente provenant de la fonction de Liouville. Plus concrètement, supposons que A soit un ensemble où λ est constant (par exemple, λ est identique -1, ce qui serait le cas si A était constitué de nombres premiers) et supposons que nous essayions d'établir une borne inférieure pour la taille de l'ensemble A dans, disons, $[N, 2N]$ en établissant une limite inférieure des sommes de diviseurs

$$1_A(n) \geq \sum_d c_d 1_{d|n}(n), \tag{7}$$

où les diviseurs d sont concentrés dans $d \leq R$ pour un niveau de crible raisonnablement petit R. Si on somme en n, on obtient une borne inférieure de la forme

$$|A| \geq \sum_d c_d \frac{N}{d} + \dots \tag{8}$$

et on peut espérer que le terme principal $d \sum_d c_d \frac{N}{d}$ sera strictement positif et le terme d'erreur est d'ordre moindre, donnant ainsi une borne inférieure non triviale sur $|A|$. Malheureusement, si on multiplie les deux côtés de (6) par le poids non négatif $1 + \lambda(n)$ et qu'on somme à n, on obtient

$$0 \geq \sum_d c_d 1_{d|n}(n)(1 + \lambda(n))$$

puisqu'on suppose λ égal à -1 sur A. Si on somme cela en n et si on utilise le fait que λ est principalement orthogonal à la somme des diviseurs, on obtient

$$0 \geq \sum_d c_d \frac{N}{d} + \dots$$

ce qui signifie essentiellement que la borne (7) ne peut pas améliorer la borne triviale $|A| \geq 0$. Un argument similaire utilisant le poids $1 - \lambda(n)$ montre également que toute borne supérieure sur $|A|$ obtenue par la théorie des cribles doit être essentiellement au moins aussi grande que $2|A|$.

Malgré ce problème de parité, il y a quelques résultats dans lesquels la théorie du crible, en conjonction avec d'autres méthodes, peut être utilisée pour compter les nombres premiers. Le premier d'entre eux est la preuve élémentaire du théorème des nombres premiers évoqué précédemment, en utilisant la structure multiplicative des nombres premiers à l'intérieur des presque premiers. Cette méthode ne semble malheureusement pas pouvoir bien se généraliser ; par exemple, le produit de deux nombres premiers jumeaux n'est pas un nombre jumeau presque premier. D'autres exemples se produisent si l'on commence à compter certaines familles spéciales à deux paramètres de nombres premiers ; par exemple, Friedlander et Iwaniec ont montré qu'il y a une infinité de nombres premiers de la forme $a^2 + b^4$ par un long argument qui a commencé avec l'identité de Vaughan, qui est en quelque sorte comme un crible exact, mais avec un terme d'erreur (non lisse) qui a la forme d'une somme bilinéaire, qui capture la corrélation avec la fonction de Liouville. La principale difficulté est de contrôler ce terme d'erreur bilinéaire, qui après un certain nombre de manipulations arithmétiques (non triviales) (en particulier, la forme $a^2 + b^4$ prise en compte sur les entiers gaussiens) se réduit à la compréhension de certaines corrélations entre la fonction de Möbius et le symbole de Jacobi, qui est ensuite réalisé par une variété d'outils de théorie des nombres. La méthode a ensuite été modifiée par Heath-Brown pour montrer également qu'il y a une infinité de nombres premiers de la forme $a^3 + 2b^3$. Les résultats connexes pour d'autres formes cubes utilisant des méthodes similaires ont depuis été obtenus par Heath-Brown et Moroz et par Helfgott (les allégations analogues pour les formes quadratiques remontent à Iwaniec). Ces méthodes semblent toutes exiger que la forme soit représentable comme une norme sur un certain champ de nombres et qu'elle ne semble donc pas encore donner une procédure générale pour résoudre le problème de parité.

Le problème de parité peut également être parfois surmonté lorsqu'il y a un zéro de Siegel exceptionnel, ce qui signifie essentiellement qu'il existe un caractère quadratique $\chi(n) = \left(\frac{n}{q}\right)$ qui est très fortement en corrélation avec les nombres premiers. Moralement parlant, cela signifie que les nombres premiers peuvent être largement récupérés à partir des P_2 presque premiers comme étant ceux presque premiers qui sont des non-résidus quadratiques modulo le conducteur q de χ, et cette information supplémentaire semble (en principe, du moins) surmonter l'obstacle de problème de parité (le fait que les zéros de Siegel, s'ils existent, réfutent GRH est lié à cela, et donc la fonction de Liouville n'est plus aussi uniformément répartie sur les ensembles lisses). Par exemple, Heath-Brown a montré que si un zéro de Siegel existait, alors il y aurait une infinité de nombres premiers jumeaux. Bien sûr, il faut supposer que les zéros de Siegel ne vérifient pas GRH, car si c'était le cas, ces résultats seraient techniquement vides ; cependant, ils suggèrent que pour briser la barrière de parité, nous pouvons supposer sans perte de généralité qu'il n'y a pas de zéro de Siegel.

Une autre façon connue de contourner partiellement le problème de la parité est de combiner des limites asymptotiques précises sur les nombres premiers (ou des fonctions de poids concentrées près des nombres presque premiers) avec une borne inférieure sur le nombre de nombres premiers, puis d'utiliser des outils combinatoires pour transformer la borne inférieure sur les nombres premiers en bornes inférieures sur des motifs de nombres premiers. Par exemple, supposons que vous sachiez

que vous pouvez compter les éléments de l'ensemble

$$A := \{n \in [N, 2N] : n, n+2, n+6 \in P_2\}$$

avec précision (où P_2 est l'ensemble des nombres presque premiers), et aussi obtenir des limites inférieures suffisamment bonnes sur les ensembles

$$A_1 := \{n \in A : n \text{ premier}\}$$

$$A_2 := \{n \in A : n+2 \text{ premier}\}$$

$$A_3 := \{n \in A : n+6 \text{ premier}\},$$

plus précisément, on obtient

$$|A_1| + |A_2| + |A_3| > |A|.$$

(À titre de comparaison, le problème de la parité prédit que l'on ne peut espérer faire mieux que de montrer cela $|A_1|, |A_2|, |A_3| \geq |A|/2$, de sorte que l'inégalité ci-dessus tombe aussi sous le coup de l'obstruction au problème de parité.)

Ensuite, juste à partir du principe des tiroirs, on déduit le fait qu'au moins deux nombres parmi $n \in [N, 2N]$ formes comme $n, n+2, n+6$ sont premiers, donnant ainsi une paire de nombres premiers dont l'écart est au plus 6. Cette approche naïve ne fonctionne pas tout à fait directement, mais en optimisant soigneusement l'argument (par exemple, en remplaçant la condition $n, n+2, n+6 \in P_2$ par quelque chose de similaire $n(n+2)(n+6) \in P_6$), Goldston, Yildirim et Pintz ont pu montrer inconditionnellement que les écarts principaux $[N, 2N]$ pourraient être aussi petits que $o(\log N)$, et pourraient en fait être aussi petits que 16 à l'infini souvent si l'on suppose vérifiée la conjecture d'Elliot-Halberstam.

Dans un esprit un peu similaire, mon résultat avec Ben Green établissant que les nombres premiers contiennent des progressions arbitrairement longues procède en utilisant d'abord des méthodes de théorie du crible pour montrer que les presque premiers (ou plus précisément, une fonction ν de poids approprié concentrée près des presque premiers) sont très pseudo-aléatoirement répartis, en ce sens que plusieurs auto-corrélations de ν peuvent être calculées et s'approcher étroitement de ce que l'on aurait prédit si les nombres presque premiers étaient répartis aléatoirement (après comptage). En raison du problème de parité, les nombres premiers eux-mêmes ne sont pas connus pour être aussi distribués de manière pseudo-aléatoire que les nombres presque premiers ; cependant, le théorème des nombres premiers nous dit au moins que les nombres premiers ont une densité relative positive parmi les nombres presque premiers. La tâche principale est alors de montrer que tout ensemble de densité relative positive dans un ensemble suffisamment pseudo-aléatoire contient des progressions arithmétiques de toute longueur spécifiée ; ce résultat combinatoire (un "théorème relatif de Szemerédi") joue à peu près le même rôle que le principe des tiroirs dans l'œuvre de Goldston-Yildirim-Pintz. (D'autre part, le théorème relatif de Szemerédi fonctionne même pour une densité arbitrairement faible, alors que le principe des tiroirs ne le fait pas ; à cause de cela, notre analyse de la théorie des cribles est beaucoup moins précise que celle de Goldston-Yildirim-Pintz.)

Il est probablement prématuré, avec notre compréhension actuelle, d'essayer de trouver un moyen systématique de contourner le problème de parité en général, mais il semble probable que nous serons en mesure de trouver d'autres moyens de contourner le problème de parité dans des cas spéciaux, et peut-être qu'une fois que nous aurons assemblé suffisamment de ces cas spéciaux, ce qu'il faut faire en général deviendra plus clair.

[**Mise à jour, 6 juin 2026** : définition de presque premier modifiée, pour préciser que tous les facteurs premiers sont importants. Référence aux entiers profinis supprimée en raison d'un conflit avec la notation établie.]