$$\frac{n^6}{72} - \frac{5n^5}{24} - \frac{1493n^4}{72} + \frac{1027n^3}{8} + \frac{100471n^2}{18} - \frac{11971n}{6} - 57347$$

> et 39, elle délivre 40 nombres premiers d'affilée: 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523 et 1601. De plus, la formule est élégante et simple, mais elle a ses limites. Pour $n = 40$, on trouve 1681... qui est 41^2.

En 2010, François Dress et Bernard Landreau en ont trouvé une meilleure, mais plus compliquée (*voir ci-dessus*). Avec ce polynôme, on obtient des nombres premiers pour n compris entre −42 et 15. La recherche de ce polynôme a tout de même demandé six mois d'efforts avec une batterie d'ordinateurs.

Est-ce donc si difficile de produire une formule qui donnerait quantité de nombres premiers? La question a été close une bonne fois pour toutes en 1947, quand William Mills a publié une formule qui peut donner un nombre arbitraire de nombres premiers. Si A = 1,306377883 8630806904686144926... alors $\lfloor A^{3^n} \rfloor$ donne une suite arbitraire de nombres tous premiers. Ici $\lfloor x \rfloor$ indique que l'on prend la partie entière du nombre x. La suite débute ainsi: 2, 11, 1361, 2521008887... Cependant, les valeurs augmentent très vite, le 8e terme a déjà 762 chiffres, et le 20e environ six milliards!

En 1951, le Britannique Edward Wright en proposait une autre, si $g_0 = \alpha = 1{,}9287800...$ et $g_{n+1} = 2^{g_n}$ alors $\lfloor g_{n+1} \rfloor = \lfloor 2^{\cdots 2^{2^\alpha}} \rfloor$ est toujours premier. Les nombres premiers consécutifs sont uniquement représentés par α. La suite obtenue est 3, 13, 16381... le 4e terme a plus de 4932 chiffres et personne n'a osé calculer le 5e...

Ainsi, ces deux suites produisent bien une infinité de nombres premiers, mais le taux de croissance décourage les plus téméraires. Peut-on élaborer des formules fournissant une suite de nombres premiers de longueur arbitraire, mais avec un taux de croissance raisonnable?

Par tous les moyens, on cherche à calculer les nombres premiers, avec une fortune diverse.

Auteur(s)	Année	Commentaire	Efficacité	Nombres calculés
Ératosthène	−276 à −194	Crible d'exclusion	Pratique	Infini calculable
Mersenne	1536	Nombres premiers de la forme 2^p-1.	Pratique, exact	51
Fermat	1640	Petit théorème de Fermat	Produit des premiers probables faibles	Infini calculable
Euler	1772	Polynôme du second degré	Pratique	40
Mills	1947	Double exponentielle	Pratique	Moins de 10
Wright	1951	Super exponentielle	Pratique	Moins de 5
Wilson	vers 1780	Formule qui utilise p!	Théorique	Très peu
Jones, Sato, Wada et Wiens	1976	Polynôme de degré 25 à 26	Théorique	Très peu
John H. Conway	1987	Fractran	Théorique	Très peu
Rowland	2008	Récurrence	Théorique	Très peu
F. Dress et B. Landreau	2010	Polynôme de degré 6	Pratique	58
Benoît Perichon *et al.*	2010	26 premiers en progression arithmétique	Pratique	26
Tomás Oliveira e Silva *et al.*	2019	Programme Primesieve: crible d'Ératosthène optimisé	Le plus rapide connu	Infini calculable sur un ordinateur actuel

LE TABLEAU DE CHASSE

Le «tableau de chasse» ci-contre récapitule des formules et des procédés pour les nombres premiers. L'infini calculable mentionné signifie que le calcul ou procédé peut se dérouler jusqu'à ce que les ressources s'épuisent. Par exemple, le programme Primesieve est le plus rapide. Il peut produire tous les nombres premiers jusqu'à 1000 milliards en 52 minutes sur un ordinateur moyen. Dans sa version courante, la liste peut aller jusqu'à 2^{64}, soit $1{,}844 \times 10^{19}$, mais les nombres réclament 4,1 exaoctets d'espace pour être stockés... Ce programme est fondé sur le crible d'Ératosthène, du nom d'un mathématicien grec du IIIe siècle avant notre ère. Cet algorithme procède par élimination: on supprime parmi les nombres de 2 à N tous les multiples d'un entier de sorte qu'à la fin il ne reste que les nombres premiers.

L'infini calculable du crible d'Ératosthène, à l'époque de son inventeur, était d'un autre ordre, et relevait plus du calcul manuel. La même chose s'applique pour le petit théorème de Fermat selon lequel si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1} - 1$ est un multiple de p. Les nombres premiers produits par ce théorème sont probables et faibles. Si p est très grand, il constitue néanmoins un test probabiliste pratique de la primalité d'un nombre candidat.

Quant aux nombres de Mersenne (de la forme $2^p - 1$), ils sont limités par la taille de p. Pour tester un seul exposant dans la liste des candidats, un voire deux mois de calcul intensif sur