Turing et les nombres premiers

Andrew R. Booker

Les exploits d'Alan Turing dans les domaines du décryptage, de la philosophie, de l'intelligence artificielle et des fondements de l'informatique sont désormais bien connus de tous. Ce que l'on sait moins, c'est que Turing s'intéressait également à la théorie des nombres, en particulier à la distribution des nombres premiers et à l'hypothèse de Riemann. Ces intérêts ont culminé dans deux programmes qu'il a mis en œuvre sur le Manchester Mark 1, le premier ordinateur numérique à programme mémorisé, au cours de ses 18 mois de fonctionnement en 1949-1950. Les efforts de Turing dans ce domaine furent modestes [1] et il convient de veiller à ne pas surestimer leur influence. Cependant, on ne peut s'empêcher de voir dans ces recherches le début du domaine de la théorie computationnelle des nombres, qui ressemble beaucoup aux problèmes actuels dans ce domaine, malgré les 60 ans qui se sont écoulés. Nous pouvons également percevoir, avec le recul, des liens frappants avec d'autres domaines d'intérêt de Turing, d'une manière qui aurait pu paraître tirée par les cheveux à son époque. Ce chapitre tentera d'expliquer les deux problèmes en détail, y compris leurs débuts, les contributions de Turing, certains développements depuis les années 1950, et des spéculations sur l'avenir.

Un peu d'histoire

Les plans de Turing pour un ordinateur. Peu de temps après la fin de son implication dans l'effort de guerre, Turing a élaboré des plans pour un ordinateur numérique à usage général. Il soumit une conception détaillée du *moteur de calcul automatique* (ACE) au Laboratoire national de physique au début de 1946. La conception de Turing s'appuyait à la fois sur le travail théorique "Sur les nombres calculables" qu'il avait mené une décennie plus tôt et sur les connaissances pratiques qu'il avait acquises pendant la guerre grâce à ses travaux à Bletchley Park, où les machines Colossus avaient été développées et utilisées. L'une des principales différences entre la conception de Turing et les ordinateurs antérieurs comme Colossus était que l'ACE devait être un *ordinateur à programme mémorisé*, ce qui signifie qu'en principe, sa programmation pouvait être modifiée rapidement, voire dynamiquement [2].

La réalisation des plans de Turing a connu plusieurs retards. Premièrement, l'existence et les capacités des machines Colossus ont été officiellement classées comme informations secrètes pendant des décennies après la guerre, de sorte qu'il a été interdit à Turing de divulguer ce qu'il savait être déjà réalisable. En conséquence, ses projets ont été jugés trop ambitieux et ont dû être réduits. Deuxièmement, Turing s'est apparemment heurté à beaucoup de bureaucratie de la part de la direction du NPL, de sorte que même la version réduite, le Pilot ACE, n'a été achevée qu'en 1950, date à laquelle Turing a démissionné de son poste du fait de sa très grande frustration.

1. Je pense que Turing lui même serait d'accord avec cela ; en effet, il ressort clairement de ses écrits de l'époque qu'il était déçu des résultats obtenus dans les deux cas.

2. Cette idée est souvent attribuée à John von Neumann, qui a contribué à la conception de deux ordinateurs contemporains de l'ACE : l'EDVAC (successeur de l'ENIAC, conçu par Eckert et Mauchly, qui avait connu un grand succès), et l'ordinateur de l'Institut pour les Études avancées à Princeton. Cependant, on ne sait pas vraiment qui est à l'origine de cette idée, ni s'il est même possible de l'attribuer à une seule personne.

Max Newman et le Manchester Mark 1. Entre temps, à la fin de 1946, l'ancien professeur de Turing à Cambridge, Max Newman, reçut une importante subvention de la Royal Society pour construire un ordinateur à l'Université de Manchester. Initialement, il devait être basé sur la conception de von Neumann pour l'ordinateur de l'IAS. Cependant, quelques mois plus tard, un effort parallèle fut lancé par Freddie Williams et son assistant Tom Kilburn au département de génie électrique de Manchester, et Newman finit par abandonner ses propres projets d'ordinateur et il rejoignit le groupe de Williams à la place. Ce fut une tournure fortuite des événements, car malgré leurs débuts tardifs, Williams et Kilburn furent les premiers à résoudre l'un des principaux défis techniques des ordinateurs à programme mémorisé : construire une banque de mémoire (ou un magasin, comme on l'appelle au Royaume Uni) qui est à la fois grand, rapide et fiable. Leur conception stockait des bits d'information sous forme de points sur un écran CRT ; il fonctionna suffisamment bien pour construire un prototype d'ordinateur fonctionnel (le SSEM, ou "Bébé") avant l'été 1948, et le Mark 1 à grande échelle fut pour l'essentiel opérationnel au bout d'un an.

Cela a laissé Newman, ainsi que deux autres mathématiciens de son groupe, I. J. Good et D. Rees, libres de réfléchir à la meilleure façon d'utiliser la nouvelle machine. Newman, un pur mathématicien, tenait apparemment à ce qu'il soit utilisé pour la recherche en algèbre et en topologie. Cela visait en partie à contraster les efforts de Manchester avec l'ACE de Turing, qui à l'époque était considéré comme l'effort majeur de la Grande Bretagne dans le domaine informatique, et qui devait être utilisé principalement pour la science appliquée (y compris peut-être pour le prochain programme britannique de bombe atomique). Après avoir démissionné de son poste au NPL, Turing commença à devenir Lecteur à Manchester à la fin de 1948, à l'invitation de Newman. Il fut chargé de diriger le développement logiciel sur le Mark 1. Good et Rees quittèrent le projet peu de temps après, laissant Turing comme principal utilisateur.

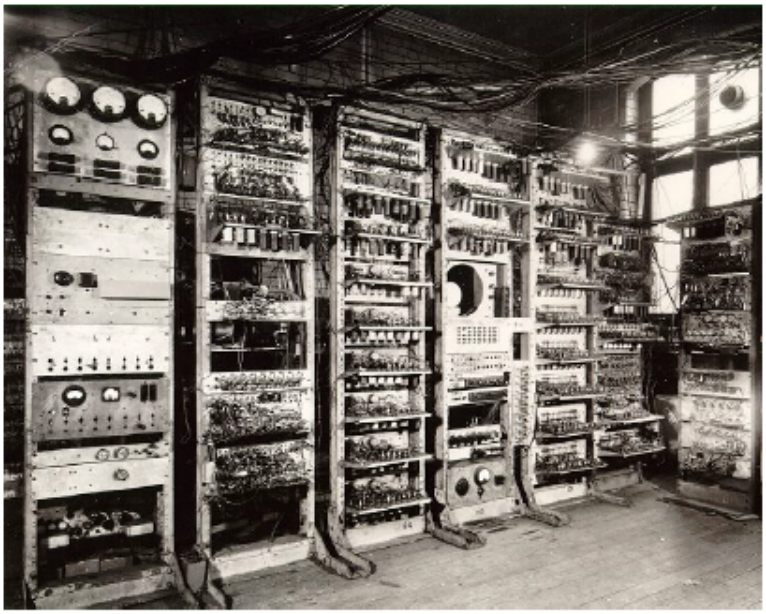

FIGURE 1. La moitié gauche du Manchester Mark 1

NOMBRES PREMIERS

Le lecteur aura peut être gardé comme souvenir de l'école primaire qu'un *nombre premier* est un entier positif qui n'est divisible que par lui-même et par 1. Demandez à n'importe quel théoricien

des nombres moderne, cependant, et vous constaterez probablement que la définition traditionnelle est évitée en faveur d'une analogie avec la chimie, dans laquelle les nombres sont comparés à des molécules et la multiplication à des réactions chimiques. Ce sont donc les nombres premiers qui jouent le rôle des atomes, ces molécules qui ne peuvent plus être décomposées (chimiquement). De la même manière que chaque molécule est une collection unique d'atomes (par exemple, chaque molécule d'eau est constituée de deux atomes d'hydrogène et d'un atome d'oxygène, donnant naissance à son symbole chimique H_2O), chaque entier positif peut s'écrire de manière unique, à changement dans l'ordre des produits près, comme produit de nombres premiers (par exemple $117 = 3^2 \times 13$). [3] Ce résultat a été suffisamment important pour les mathématiciens du XIX$^{\text{e}}$ siècle pour qu'ils l'appellent le *Théorème Fondamental de l'Arithmétique* (FTA). [4]

Les gens s'intéressent aux nombres premiers depuis au moins les Grecs de l'Antiquité. Euclide a enregistré une preuve qu'il en existe une infinité vers 300 avant JC [10, § 1.1.2]. Sa preuve, qui reste l'une des plus élégantes preuves des mathématiques, peut s'exprimer sous la forme d'un algorithme :

(1) Écrivez quelques nombres premiers.
(2) Multipliez-les ensemble et ajoutez 1 ; appelons le résultat n.
(3) Trouvez un facteur premier de n.

Par exemple, si nous savons que 2, 5 et 11 sont tous premiers, alors en appliquant l'algorithme avec ces nombres, on obtient $n = 2 \times 5 \times 11 + 1 = 111$, qui est divisible par le nombre premier 3. Par un théorème antérieur des *Éléments* d'Euclide, le nombre n calculé à l'étape (2) doit avoir un facteur premier (et en fait, il peut être factorisé de manière unique en un produit de nombres premiers par le théorème fondamental de l'arithmétique), donc l'étape (3) est toujours possible. En revanche, d'après la façon dont Euclide construit le nombre n, le facteur premier trouvé à l'étape (3) ne peut être aucun des nombres premiers notés à l'étape (1). Par conséquent, la liste des nombres premiers ne peut être complète, c'est à dire qu'il y en a une infinité.

Notons que n peut avoir plus d'un facteur premier (par exemple, le nombre 111 dans notre exemple est également divisible par 37), et Euclide ne précise pas lequel prendre à l'étape (3). En 1963, Albert Mullin a rendu la preuve d'Euclide complètement constructive en commençant avec juste le nombre premier 2 et en répétant l'algorithme pour ajouter un nouveau facteur premier à la liste, en choisissant toujours le plus petit facteur premier de n à l'étape (3). De façon similaire, on peut toujours choisir le plus grand facteur premier, et ces deux constructions ont pour résultat ce qu'on appelle des *séquences d'Euclide-Mullin* de nombres premiers [10, § 1.1.2], dont les premiers termes sont présentés dans le tableau 1. Mullin a posé la question naturelle de savoir si *tout* nombre

3. Il y a un long débat, entre amateurs et mathématiciens professionnels, pour savoir si 1 devrait être ou pas considéré comme un nombre premier. Dans l'analogie chimique, 1 (qui est ce que l'on a, avant de multiplier par quoi que ce soit) est comme l'espace vide (qui est ce que l'on a, avant l'introduction d'un quelconque atome). Donc, puisque cela satisfait la définition de nombre premier donnée ci-dessus d'un point de vue puritain, cela ne satisfait clairement pas l'esprit de l'analogie. De plus, faire de 1 un nombre premier causerait des ravages dans l'unicité de la factorisation en nombres premiers, puisque toute factorisation pourrait inclure un nombre arbitraire de 1. Pour éviter cette pathologie, la convention moderne est de considérer 2 comme étant le premier nombre premier, et de modifier la définition en conséquence.

4. L'approche la plus commune pour prouver le FTA remonte à Euclide, mais il a fallu attendre le travail de Gauss en 1801 pour qu'il soit insisté sur ce point de vue et qu'une preuve complète ne soit donnée.

premier finit par apparaître dans chaque séquence. On n'a toujours pas la réponse à cette question pour la première séquence, bien qu'on ait conjecturé que la réponse est oui.

première séquence (plus petit facteur premier)	seconde séquence (plus grand facteur premier)
2	2
3	3
7	7
43	43
13	139
53	50207
5	340999
6221671	2365347734339
38709183810571	4680225641471129
139	1368845206580129

TABLE 1. Les dix premiers termes des séquences d'Euclide-Mullin

D'un autre côté, il a été démontré récemment (en 2011) qu'il manque une infinité de nombres premiers dans la seconde séquence. Cela montre que même de très anciens problèmes de théorie des nombres peuvent engendrer des recherches intéressantes.

Euclide a été suivi un siècle plus tard par Ératosthène, qui a trouvé l'algorithme de recensement des nombres premiers qui est toujours d'usage aujourd'hui. Ces résultats sont typiques des méthodes contrastées utilisables pour étudier et utiliser les nombres premiers : soit en les regardant individuellement (comme dans le cas d'Ératosthène), ou bien en essayant de comprendre des propriétés générales de la séquence de tous les nombres premiers, même ceux qui sont bien au-delà de notre capacité de calcul (comme dans le cas d'Euclide). Comme on le verrai, les deux programmes de Turing sur le Manchester Mark 1 appartiennent carrément à ces deux champs respectifs.

Grands nombres premiers

Le premier de ces deux programmes était une idée de Newman, conçue comme une manière de tester les capacités de la nouvelle machine et de faire de la publicité pour le projet. Il s'agissait de chercher un grand nombre premier.

Nombres premiers de Mersenne. De la même façon qu'il y a un élément le plus notoire pour chaque instant de l'Histoire, il y a aussi un nombre premier connu le plus grand. Au moment de l'écriture de cet article, le plus grand nombre premier connu est $2^{57\,885\,161} - 1$, un nombre avec plus de 17 millions de chiffres, mais ce record ne tiendra pas longtemps. Ceci est un exemple de *nombre premier de Mersenne*, ceux-ci étant de la forme une puissance de deux moins 1. On les appelle ainsi du nom d'un moine français Marin Mersenne, qui en 1644 prédit que $2^n - 1$ est premier pour $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, et pour aucune autre valeur de $n < 258$. Tous sauf les quatre derniers étaient connus au moment de sa conjecture, et on sait qu'il s'est trompé pour 67 et 257 et qu'il a oublié $n = 61, 89$ et 107, qui fournissent également des nombres premiers. Le nom est resté cependant !

Dans l'histoire récente (les 150 dernières années à peu près), le nombre premier le plus grand est habituellement un nombre premier de Mersenne. Cela est probablement dû au fait qu'il s'avère un

peu plus facile de trouver des nombres premiers parmi les nombres de Mersenne que pour des classes de nombres plus générales, et de ce fait, ils ont reçu davantage d'attention, pour quelques raisons. D'abord, il n'est pas difficile de voir que si $2^n - 1$ est un nombre premier alors n lui-même doit être un nombre premier, ce qui permet d'éliminer la plupart des nombres composés. (Malheureusement, ce test ne fonctionne que dans un sens, i.e. lorsque n est un nombre premier, il n'est pas obligatoire que $2^n - 1$ en soit un ; le plus petit contre-exemple est $2^{11} - 1 = 2047 = 23 \times 89$.) Deuxièmement, il y a un algorithme très rapide, décrit par Lucas en 1876 puis plus tard amélioré par D. H. Lehmer, pour tester la primalité d'un candidat donné $2^n - 1$ quand n est un nombre premier supérieur à 2 :

(1) Commencer avec le nombre $x = 4$.
(2) Remplacer x par le reste de la division de $x^2 - 2$ par $2^n - 1$.
(3) Répéter l'étape (2) $n - 2$ fois.
(4) Alors $2^n - 1$ est un nombre premier si la valeur terminale de x est 0, et c'est un nombre composé sinon.

(Le lecteur est invité à essayer cela avec $n = 3$ ou $n = 5$. Avec du papier et une calculette à disposition, c'est aussi marrant de tester que le test prouve correctement que $2^{11} - 1$ n'est pas un nombre premier.) Troisièmement, la forme des nombres de Mersenne (une puissance de 2 moins 1) rend l'arithmétique du test de Lucas-Lehmer particulièrement aisée à mettre en œuvre sur ordinateur, puisque les calculs internes sont effectués en binaire.

Une autre raison d'étudier les nombres premiers de Mersenne est leur connexion avec ce qu'on appelle les *nombres parfaits*, qui sont ces nombres qui sont égaux à la somme de leurs diviseurs propres. Par exemple, les diviseurs propres de 28 sont 1, 2, 4, 7 et 14, et leur somme vaut 28. Ces nombres ont aussi été étudiés depuis l'Antiquité, et en fait, Euclide savait déjà que si $p = 2^n - 1$ est un nombre premier alors $p(p + 1)/2$ est un nombre parfait ; par conséquent, par exemple, le nombre parfait $28 = 7 \times 8/2$ noté ci-dessus est relié au nombre premier de Mersenne $7 = 2^3 - 1$, et chaque nouveau nombre premier de Mersenne qui est également trouvé amène avec lui un nouveau nombre parfait. (Incidemment, $p(p + 1)/2$ est aussi la somme des nombres de 1 à p, par exemple $28 = 1+2+3+4+5+6+7$, donc il n'est pas étonnant que les mathématiciens antiques aient pensé que ces nombres avaient des propriétés mystiques comparés aux nombres ordinaires, au point de les qualifier de "parfaits") Environ 2000 ans plus tard, Euler a prouvé l'assertion inverse que tout nombre parfait pair provient de la construction d'Euclide, et qu'il y a donc une correspondance directe entre les nombres premiers de Mersenne et les nombres parfaits pairs. On ne sait toujours pas s'il existe un nombre parfait impair, bien qu'on croit en général qu'il n'en existe pas.

Les nombres premiers de Mersenne à l'ère électronique. En 1947 environ, tous les nombres de Mersenne $2^n - 1$ pour n jusqu'à 257 avaient été testés à la main, confirmant la conjecture originale de Mersenne. Le plus grand nombre premier parmi ceux-ci était $2^{127} - 1$, découvert par Lucas en 1876. Tous les nombres premiers depuis lors ont été découverts par des ordinateurs. (Pourtant, Ferrier a découvert que $(2^{148} + 1)/17$ est un nombre premier en 1951 en utilisant seulement une calculatrice de bureau ; ce nombre reste le nombre premier le plus grand découvert "à la main".) Une première telle investigation a été faite par Turing, avec Newman et les ingénieurs Tom Kilburn et Geoff Tootill, pendant l'été 1949. À partir d'une lettre [5] que Turing écrivit à D. H. Lehmer en mars

5. trouvé dans le fond d'archives d'Emma et D. H. Lehmer Archive à la Bibliothèque Bancroft, UC Berkeley.

1952, on sait que l'équipe vérifia tous les nombres premiers de Mersenne connus et que la recherche fut étendue jusqu'à $n = 433$, bien que Turing ait décrit leurs efforts comme non systématiques. Finalement, le test amena de la publicité que Newman souhaitaità la nouvelle machine, mais cette publicité s'arrêta rapidement, puisqu'ils stoppèrent la recherche avant d'avoir trouvé de nouveaux nombres premiers.

La valeur scientifique de leur travail peut faire débat à cause de cela, bien que même s'ils avaient trouvé un nouveau nombre premier, cela serait maintenant juste une note de bas de page dans l'histoire. Dans tous les cas, il ne s'écoula pas longtemps avant que de nouveaux records de nombres premiers ne soient découverts par ordinateur ; Miller et Wheeler en trouvèrent plusieurs nouveaux en 1951 en utilisant le EDSAC à Cambridge, et Robinson trouva les cinq nombres premiers de Mersenne suivants en 1952 en utilisant le SWAC au Bureau National des Standards à Los Angeles. Le calcul de Robinson, décrit en détail par Corry [4], est particulièrement impressionnant puisque il a écrit son programme en n'ayant jamais vu d'ordinateur avant cela. Il envoya les cartes contenant le code par mail à D. H. et Emma Lehmer à Los Angeles. Ils ont fait tourner le programme pour la première fois le 30 janvier 1952 ; il s'est exécuté sans bug et il a trouvé le prochain nombre premier de Mersenne, $2^{521} - 1$, le même jour. Turing exprima combien il était impressionné par les résultats de Robinson dans sa lettre à D. H. Lehmer.

La recherche de nombres premiers de Mersenne s'est poursuivie sans relâche depuis lors. Cela présume, bien sûr, qu'il y en a davantage à trouver ; pourtant, il n'y a pas d'analogue de la preuve d'Euclide pour les nombres premiers de Mersenne, et malgré une évidence heuristique claire, ainsi qu'empirique, nous n'avons toujours pas de preuve qu'il y en a une infinité. Au jour du présent article, 36 d'entre eux ont été trouvés par ordinateur [6]. Depuis le milieu des années 1990, la recherche a été dominée par la bien nommée Great Internet Mersenne Prime Search, conçue par l'informaticien George Woltman. Le programme de Woltman utilise le temps disponible d'ordinateurs de milliers de volontaires, reliés par l'internet [7]. Ils ont découvert de nouveaux nombres premiers records du monde au rythme d'environ un par an.

Les tests de primalité en général et la cryptographie à clef publique. Le célèbre mathématicien et pacifiste G. H. Hardy écrivit en 1940 que

> Personne n'a jamais découvert qu'un quelconque objectif militaire ait été atteint par la théorie des nombres ou la relativité, et il semble peu probable que quiconque n'en atteigne un pour de nombreuses années encore.

Hardy voyait la théorie des nombres comme la "plus pure" des disciplines, non entachée par la nécessité d'avoir des applications. Avec ce point de vue à l'esprit, il n'est pas surprenant que Newman ait choisi une recherche de nombres premiers pour inaugurer la machine qu'il destinait à un usage en mathématiques pures.

6. Cette phrase fait surgir une question philosophique : devrait-on créditer un ordinateur de la découverte avec les personnes qui ont écrit et exécuté son programme ? Un cas particulièrement intéressant a eu lieu le 12 avril 2009, quand un ordinateur a démontré que le nombre $2^{42\,643\,801} - 1$ est un nombre premier, faisant de ce nombre le troisième plus grand nombre premier de Mersenne connu ; pourtant, personne n'a remarqué ce fait jusqu'au 4 juin de cette année. Cette date devrait-elle être considérée comme la date de la découverte ?

7. La lectrice est invitée à participer ; visiter www.mersenne.org pour obtenir des détails.

Avec une sagesse rétrospective, les remarques de Hardy sont un peu ironiques. La compréhension de la relativité restreinte a amené au développement des armes nucléaires seulement quelques années après ses écrits. Comme pour la théorie des nombres, et pour l'étude des nombres premiers en particulier, on pourrait de façon plausible arguer de l'opinion de Hardy jusqu'à la fin des années 1970 et l'avènement de la cryptographie à clef publique. Pour expliquer ces derniers termes, on sait maintenant qu'il est théoriquement possible pour deux personnes qui ne se sont jamais rencontrées ou même qui n'ont jamais communiqué précédemment de se trouver à deux extrêmes opposées d'une pièce bondée et de s'envoyer des messages l'un à l'autre en totale confidentialité en utilisant une paire de mégaphones [8].

Le cryptosystème à clef publique le plus fréquemment déployé est RSA, inventé par Rivest, Shamir et Adleman en 1978 [9]. Il repose de façon cruciale sur le fait qu'il est facile de multiplier deux nombres premiers ensemble mais, jusqu'à présent, il est très difficile de déterminer quels nombres premiers ont été multipliés quand on donne leur produit, même si le FTA garantit qu'il y a une réponse unique [10].

Cela aurait pu être désastreux pour les Alliés car si des systèmes de cryptographie à clef publique avaient été utilisés pendant la guerre, il est vraisemblable que même des cerveaux aussi intelligents que celui de Turing n'auraient pas été capables de casser les codes. Pourtant, aujourd'hui, c'est généralement regardé comme une bonne chose, et certains peuvent même considérer que c'est essentiel à la vie moderne. Un exemple qui est moins absurde qu'une pièce équipée de mégaphones mais assez proche de cette idée, c'est la sécurisation des connexions internet, qui démarre habituellement avec le cryptosystème RSA. C'est pourquoi, par exemple, on peut se sentir en sécurité en envoyant notre numéro de cartes de crédit à un site internet à travers le réseau internet public.

Une ride dans cette théorie est que nous n'avons aucune preuve que la sécurité des cryptosystèmes à clef publique habituellement connus ne peut être facilement cassée, ou même qu'un tel système existe *en principe* ; c'est le fameux problème P vs. NP, soi-disant le problème le plus important non résolu en informatique. Pour tempérer les effets potentiellement calamiteux de la casse d'un tel cryptosystème, les chercheurs ont créé de nombreux systèmes différents qui ne sont pas liés de façon évidente les uns aux autres, de telle façon qu'il n'y ait pas de pénurie de possibilités de substitutions si, par exemple, quelqu'un découvrait un moyen rapide de factoriser les nombres. Pourtant, ceci n'exclut pas la panique tant que des systèmes de remplacement ne seront pas entièrement déployés [11].

Les chercheurs se mettent également fréquemment à la place des attaquants, pour tester la force des différents cryptosystèmes. Ainsi, l'algorithme RSA a engendré de l'intérêt à la fois pour les tests de

8. On ne suggère pas que cela soit mis en pratique.

9. Un système similaire a été décrit cinq ans plus tôt par Clifford Cocks de GCHQ, mais est resté secret jusqu'en 1998.

10. Les preuves que l'on a du FTA sont toutes des preuves d'*existence*, i.e. elles affirment que tout nombre a une factorisation en nombres premiers unique mais ne fournissent pas d'information utile sur la manière de la trouver.

11. Un autre problème est que l'on pense que les systèmes de cryptage à clef publique actuels seraient tous vulnérables à l'attaque si de grands *ordinateurs quantiques* étaient développés. Pourtant avec les ordinateurs quantiques vient également la promesse de méthodes encore plus fortes de transmission sûre de l'information, des méthodes qui rendent théoriquement impossible l'interception de l'information.

primalité, i.e. des algorithmes pour décider si un nombre donné est un nombre premier ou pas, et dans la factorisation. Du côté théorique, il a finalement été démontré en 2002 par Agrawal, Kayal et Saxena que le test de primalité est par exemple "facile" pour des nombres d'une forme quelconque [12], même si les algorithmes qui sont plus rapides en pratique étaient déjà connus. En termes pratiques, quiconque disposant d'un PC haut de gamme acheté de nos jours peut télécharger un logiciel gratuit qui peut rapidement prouver la primalité de nombres qui ont des milliers de chiffres, et factoriser un nombre de 100 chiffres environ en une journée. La difficulté de la factorisation augmente rapidement avec la taille, donc par exemple factoriser des nombres quelconques de 230 chiffres est couramment possible, mais seulement avec un investissement conséquent en temps et en argent. Les implémentations typiques de RSA en usage de nos jours emploient des nombres avec au moins 1024 bits (environ 300 chiffres), bien que cette taille minimum soit amenée à augmenter au fur et à mesure que s'amélioreront la puissance de calcul et des algorithmes.

La distribution des nombres premiers

Le second problème que Turing étudia sur le Manchester Mark 1 était l'hypothèse de Riemann (ou HR), qui a à voir avec la distribution asymptotique des nombres premiers. C'était un problème cher au cœur de Turing, et en fait, il fit une première tentative de recherche au sujet de HR en 1939 avec une machine analogique à but dédié, en utilisant un système sophistiqué d'engrenages. Turing avait apparemment coupé la plupart des engrenages de la machine avant d'être interrompu par la guerre. Lorsqu'il put revenir à ce problème, en juin 1950, on avait fait de tels progrès sur les ordinateurs digitaux généralistes que la machine de Turing de 1939 était devenue obsolète. (La machine ne fut jamais terminée, bien qu'on ait un article témoignant de sa construction par l'ami de Turing Donald McPhail. Un projet a récemment été lancé pour la construire ; ironiquement, la première étape de cette entreprise sera une simulation informatique.) En effet, il est devenu courant, ne serait-ce qu'à peine, de considérer plus de choses que ce qu'il était possible de faire avec une machine analogique testant algorithmiquement HR, sans intervention humaine. Comme nous le verrons ci-dessous, cet aspect du problème, souvent pris pour acquis dans les discussions modernes du sujet, était d'un vif intérêt pour Turing.

L'histoire derrière l'hypothèse de Riemann remonte à Gauss, qui à 15 ou 16 ans (en 1792-1793) faisait de longues listes de nombres premiers dans le but de juste comprendre à quelle fréquence ils apparaissent. (On peut clairement dire que Gauss était un calculateur théoricien des nombres avant même qu'il y ait des ordinateurs !) Il vint à conjecturer qu'autour du nombre x, grossièrement un nombre sur ln nombres entiers est un nombre premier [13] ; par conséquent, si l'on souhaite savoir combien il y a de nombres premiers parmi les nombres 2, 3, 4, ..., x (sans les compter effectivement), on peut estimer cela par l'intégrale $\int_2^x \frac{1}{\ln t} dt$, que l'on dénote habituellement $\mathrm{Li}(x)$. On peut appeler cela la version quantitative du résultat qualitatif d'Euclide qui énonce qu'il y a une infinité de nombres premiers.

12. par opposition aux tests testant la primalité de nombres d'une forme particulière, tels que le test de Lucas-Lehmer pour les nombres de Mersenne, qu'on a utilisé longtemps.

13. Ici, ln dénote le logarithme naturel, de base $e = 2.71828...$.

x	$\pi(x)$	nombre entier le plus proche de $\mathrm{Li}(x)$
1000	168	177
10^6	78 498	78 627
10^{12}	37 607 912 018	37 607 950 280
10^{24}	18 435 599 767 349 200 867 866	18 435 599 767 366 347 775 143

TABLE 2. Comparaison de $\pi(x)$ vs. $\mathrm{Li}(x)$

La Table 2 montre le nombre de nombres premiers jusqu'à x, habituellement dénoté par la lettre $\pi(x)$ (bien que cela n'ait rien à voir avec la constante $\pi = 3.14159...$), pour différentes puissances de 10. On voit également dans la table le nombre entier le plus proche de l'approximation de Gauss $\mathrm{Li}(x)$. Une chose qui est immédiatement apparente est que $\mathrm{Li}(x)$ semble donner une surestimation de la valeur effective, et en fait qui est correcte pour toute valeur de $\pi(x)$ pour x supérieur à 8 qui ait été calculée jusque-là. On pensa quelques temps qu'il devait toujours être vrai que $\mathrm{Li}(x) > \pi(x)$ pour de grandes valeurs de x, mais Littlewood prouva en 1914 que ceci est faux pour certains x, et que de plus, la direction de l'inégalité varie une infinité de fois. En 1933, Skewes prouva le théorème de Littlewood en montrant que le premier changement de signe a lieu avant $x = 10^{10^{10^{34}}}$ si l'hypothèse de Riemann non encore démontrée (dont il a été question ci-dessus) était vraie. Ce nombre est inimaginablement grand, c'est pourquoi Hardy l'appela "le plus grand nombre qui ait jamais servi à aucun objectif défini en mathématiques." (Cela aurait pu être vrai en 1933, mais des mathématiciens ont depuis trouvé des moyens d'utiliser des nombres beaucoup plus grands, comme ceux qu'on trouve dans la *théorie de Ramsey*.)

Turing travailla à l'amélioration de l'argument de Skewes, espérant réduire la borne significativement et il réussit à supprimer l'hypothèse concernant HR [7, 8]. Il fit des progrès par rapport à ces deux objectifs à l'été 1937, et il revint à ce problème environ en 1952-1953, mais il ne publia jamais son travail. Dans tous les cas, à la fois les approches de Skewes et de Turing ont depuis été supplantées par un travail ultérieur basé sur des méthodes computationnelles ; on discutera de ces derniers résultats ci-après.

La fonction zeta de Riemann. La fonction zeta de Riemann est la série infinie

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Comme on l'apprend en cours de calcul, cette série converge pour tout $s > 1$ et diverge pour tout $s \leq 1$; le cas limite $s = 1$ est celui de la célèbre *série harmonique*, $\sum_{n=1}^{\infty} \frac{1}{n}$. La connexion entre la fonction zeta et les nombres premiers vient d'une autre formule pour $\zeta(s)$, dérivée par Euler en 1737 [10, § 1.1.4] :

$$\zeta(s) = \frac{1}{1 - \frac{1}{2^s}} \times \frac{1}{1 - \frac{1}{3^s}} \times \frac{1}{1 - \frac{1}{5^s}} \times \ldots = \prod_{p \text{ premier}} \frac{1}{1 - \frac{1}{p^s}}.$$

Ici, elle est donnée comme un produit infini plutôt que comme une somme, et la variable p couvre tous les nombres premiers (2, 3, 5, 7, 11, ...).

L'équivalence entre (1) et (2) est une sorte d'expression analytique du théorème fondamental de l'arithmétique mentionné précédemment. Pour voir cela, on développe d'abord le facteur $\frac{1}{1-\frac{1}{p^s}}$ en utilisant la formule pour une série géométrique :

$$\frac{1}{1-\frac{1}{p^s}} = 1 + \frac{1}{p^s} + \left(\frac{1}{p^s}\right)^2 + \left(\frac{1}{p^s}\right)^3 + \ldots = 1 + \frac{1}{p^s} + \frac{1}{(p^2)^s} + \frac{1}{(p^3)^s} + \ldots$$

Ensuite, on multiplie ces séries géométriques pour tous les choix de p. Pour faire cela, on doit imaginer tout produit concevable de termes $\frac{1}{(p^k)^s}$ pour différents nombres premiers p et des exposants k. Par exemple, un terme qui apparaît est $\frac{1}{(3^2)^s} \times \frac{1}{13^s} = \frac{1}{117^s}$, venant des termes correspondant pour $p = 3$ et $p = 13$. Plus généralement, il n'est pas difficile de voir que tout produit de termes prendra la forme $\frac{1}{n^s}$ pour un certain entier positif n. En fait, pour n'importe quel n donné, le terme $\frac{1}{n^s}$ doit finalement apparaître, puisque n a une certaine factorisation en nombres premiers. Finalement, puisque la factorisation en nombres premiers de n est unique, $\frac{1}{n^s}$ apparaît exactement une seule fois. Ainsi, on arrive à la série définie originellement.

Toutes ces manipulations font sens et peuvent être rendues complètement rigoureuses à chaque fois que $s > 1$. Euler avait eu l'idée lumineuse de faire tendre s vers 1, de telle façon que (1) tende vers la série harmonique, qui diverge [14]. Ainsi, le cas peut également se produire où (2) devient arbitrairement grand lorsque s s'approche de 1. À partir de cela [15], Euler conclut qu'il y a une infinité de nombres premiers p puisque sinon, (2) aurait du sens et resterait borné et pair lorsque s s'approche de 1. Cette preuve, quoique diaboliquement intelligente, peut sembler bien plus compliquée qu'elle ne l'est effectivement étant donné qu'Euclide a déjà démontré qu'il y avait une infinité de nombres premiers il y a deux mille ans environ. Ce qui rend la démonstration d'Euler importante, c'est qu'elle peut être généralisée de différentes manières alors que la preuve d'Euclide ne peut pas être généralisée.

D'abord, en 1837, Dirichlet a montré comment modifier la preuve d'Euler pour montrer qu'une progression arithmétique

$$a, a + b, a + 2b, a + 3b, ...,$$

contient un nombre infini de nombres premiers tant que a et b n'ont pas de facteur commun [10, § 2]. (Si a et b ont un facteur commun alors il est facile de voir que cette progression peut contenir au moins un nombre premier ; par exemple, la progression 6, 10, 14, 18, ... ne contient pas de nombre premier puisque tous ses termes sont pairs.) Pour faire cela, il a introduit certaines versions modifiées de la fonction zeta, les fonctions appelées "fonctions L" qui portent maintenant son nom, et il a à nouveau étudié leur comportement lorsque s tend vers 1. Le théorème de Dirichlet est important au sens où il a été utilisé comme ingrédient dans un nombre incalculable d'autres théorèmes

14. Ceci est une interprétation moderne de son argument ; au XVIII^{e} siècle, les notions de limite et de convergence n'étaient pas encore formulées rigoureusement, donc Euler aurait plus franchement rendu s égal à 1 et ne se serait pas trop préoccupé du fait que cela fasse sens de procéder ainsi. Le pendulum peut également tourner dans l'autre sens ; le sujet de l'*analyse non-standard* permet une formulation rigoureuse de l'approche plus directe d'Euler bien que, comme son nom l'implique, elle ne soit pas encore totalement acceptée par tous les mathématiciens.

15. Une version alternative, populaire parmi les théoriciens algébriques des nombres, est de considérer à la place $s = 2$. Un autre théorème d'Euler dit que $\zeta(2) = \pi^2/6$, et s'il y avait seulement un nombre fini de nombres premiers alors, par (2), ce nombre serait rationnel. Pourtant, Legendre a démontré en 1794 que π^2 (et par conséquent également $\pi^2/6$) est irrationnel.

de la théorie des nombres. De plus, il marque le début de ce que l'on appelle maintenant *la théorie analytique des nombres*, qui utilise des techniques de l'analyse réelle et de l'analyse complexe pour étudier des questions fondamentales au sujet des nombres.

Deuxièmement, en 1859, Riemann écrivit un article pionnier sur la fonction zeta, son unique article relié à la théorie des nombres [10, § 4]. Dans celui-ci, il décrivit la manière dont une étude détaillée de $\zeta(s)$ (cette notation a été introduite par Riemann) peut être utilisée pour voir non seulement qu'il y a une infinité de nombres premiers, mais également pour comprendre leur distribution asymptotique, amenant finalement à des preuves d'une conjecture de Gauss qui furent amenées indépendamment par Hadamard et par de la Vallée Poussin en 1896 ; on appelle maintenant ce résultat les *théorème des nombres premiers* [12]. L'idée clef de Riemann était de considérer $\zeta(s)$ non pas seulement pour des nombres réels s, mais également pour des nombres s complexes. En fait, il a montré, à travers le principe du prolongement analytique, comment $\zeta(s)$ pouvait avoir du sens pour tous les nombres complexes s à part 1. Le point crucial s'est avéré être la compréhension des valeurs de s pour lesquelles $\zeta(s) = 0$. On sait que $\zeta(s)$ s'annule pour $s = -2, -4, -6, ...$, et pour une infinité de valeurs non réelles de s de partie réelle comprise entre 0 et 1. Riemann a calculé des approximations de quelques-uns des premiers zéros non réels, qui sont fournis dans la Table 3. (Les zéros adviennent par paires de nombres complexes conjugués, i.e. à tout zéro en $x + iy$, il en correspond un autre en $x - iy$. Ainsi, il suffit de lister ceux qui sont de partie imaginaire positive). Riemann a alors émis la supposition audacieuse que tous ont une partie réelle exacte (égale à 0.5).

$0.5+i$ 14.134725141734693790 45...
$0.5+i$ 21 :022039638771554992 62...
$0.5+i$ 25 :010857580145688763 21...
$0.5+i$ 30 :424876125859513210 31...
$0.5+i$ 32 :935061587739189690 66...

Pourquoi les . sont-ils devenus des : ???

TABLE 3. Les cinq premiers zéros de la fonction zeta de Riemann et leur partie imaginaire positive

On n'est toujours pas assuré de cette supposition, maintenant appelée Hypothèse de Riemann [3], plus de 150 ans après, bien qu'il y ait une évidence significative en sa faveur, et la plupart des mathématiciens d'aujourd'hui croient que l'hypothèse de Riemann est vraie. Si elle est vraie, HR implique que l'estimation de Gauss sur le nombre de nombres premiers jusqu'à x est précise à l'"ordre de la racine carrée", ce qui, en d'autres termes, signifie que grosso-modo, la moitié supérieure des chiffres de l'estimation sont corrects ; par exemple, alors qu'il est bien en-deçà de notre technologie de dire exactement combien il y a de nombres premiers avec au plus 50 chiffres, la formule de Gauss prédit qu'il y en a environ

$$\underline{87626803175078416887817}6862640406870986031109950,$$

et il est vraisemblable que les chiffres soulignés soient corrects. En l'absence d'une preuve de HR, on a pu trouver des résultats plus faibles ; par exemple, on sait de façon sûre que le nombre de chiffres corrects dans l'approximation de Gauss augmente avec le nombre de chiffres de x (ce qui est l'énoncé qualitatif du théorème des nombres premiers), mais l'on ne sait toujours pas si cette variation est linéaire.

Turing et l'hypothèse de Riemann. Une chose qui fait de HR une bonne conjecture, c'est sa falsifiabilité, i.e. il suffirait de trouver un contre-exemple pour montrer clairement qu'elle est fausse.

Il y a plusieurs raisons philosophiques de croire à la vérité de HR, mais à part cela, la plus grande évidence que l'on a en sa faveur est le grand nombre de tests numériques qui ont été faits, dont aucun ne s'est avéré faux. (D'un autre côté, comme le montre la question $\pi(x)$ vs. $\mathrm{Li}(x)$, on ne devrait pas se reposer complètement sur l'évidence numérique). Curieusement, Turing n'était pas convaincu de la véracité de l'hypothèse de Riemann ; par exemple, il est clair dans son article sur le sujet [11] qu'il avait espéré que le Manchester Mark 1 trouverait un contre-exemple. Pour sa défense, le scepticisme au sujet de la conjecture n'était pas commun dans la première moitié du XX^e siècle, et des presque contre-exemples trouvés lors des premières recherches firent penser qu'un peu plus de calculs permettraient de trouver un véritable contre-exemple.

Comme mentionné ci-dessus, le premier calcul de ce type fut effectué par Riemann lui-même [16], et il figura probablement dans sa formulation de la conjecture. Dans les années 1930, Titchmarsh avait étendu les calculs jusqu'à plus de 1000 zéros, qui tous vérifiaient HR. La méthode de Titchmarsh qui était essentiellement dérivée de celle de Riemann consistait en deux étapes principales :

(1) Trouver tous les zéros de partie réelle $\frac{1}{2}$ et de partie imaginaire comprise entre 0 et un certain grand nombre T. Bien que les valeurs de $\zeta(\frac{1}{2}+it)$ pour les nombres réels t soient typiquement complexes, il s'avère que l'on peut définir une fonction à valeurs réelles $Z(t)$ avec la même valeur absolue que celle de $\zeta(\frac{1}{2}+it)$. Ainsi, les zéros de $Z(t)$ correspondent aux zéros de la fonction zeta de Riemann de partie réelle $\frac{1}{2}$, et on peut les trouver simplement en inspectant le graphe de $Z(t)$ et en notant où il croise l'axe de t (voir la Figure 2, partie haute).
(2) Trouver, par un calcul auxiliaire, le nombre total, disons $N(T)$, de zéros non réels de la fonction zeta de partie imaginaire allant jusqu'à T. Si cela est en accord avec le comptage des zéros de partie réelle trouvé dans l'étape (1) alors tous les zéros de partie imaginaire jusqu'à T satisfont HR.

De ces deux étapes, la première est relativement évidente. En fait, Riemann avait déjà trouvé une formule (publiée plus tard par Siegel) qui pourrait être utilisée pour évaluer $Z(t)$ très rapidement, qu'il utilisa pour ses calculs. La seconde étape est un grand défi plus compliqué ; les méthodes utilisées dans toutes les investigations jusqu'à une certaine valeur et incluant les idées de Titchmarsh étaient ad hoc et il n'était pas garanti qu'elles fonctionnent pour de grandes valeurs de T. Cela n'était pas assez bon pour Turing, qui voulait que les machines travaillent d'une manière aussi autonome que possible. À la place, il trouva un critère qui pourrait être utilisé pour décider si tous les zéros avaient bien été trouvés *en utilisant les valeurs qui avaient déjà été calculées*. Ainsi, Turing remplaça effectivement l'étape la plus lourde dans la vérification par un test automatique.

La méthode de Turing était basée sur une comparaison vigilante des valeurs observées de $N(T)$ versus sa propre formule asymtotique lorsque T augmente. Riemann postula, et il fut plus tard rigoureusement démontré que cette fonction $N(T)$ pouvait être approximée par une fonction lisse

$$M(T) = \frac{T}{2\pi}\ln\left(\frac{T}{2\pi e}\right) + \frac{7}{8}.$$

16. Ceci fut seulement découvert des décades après la mort de Riemann en examinant ses notes non publiées dans la bibliothèque de Göttingen.

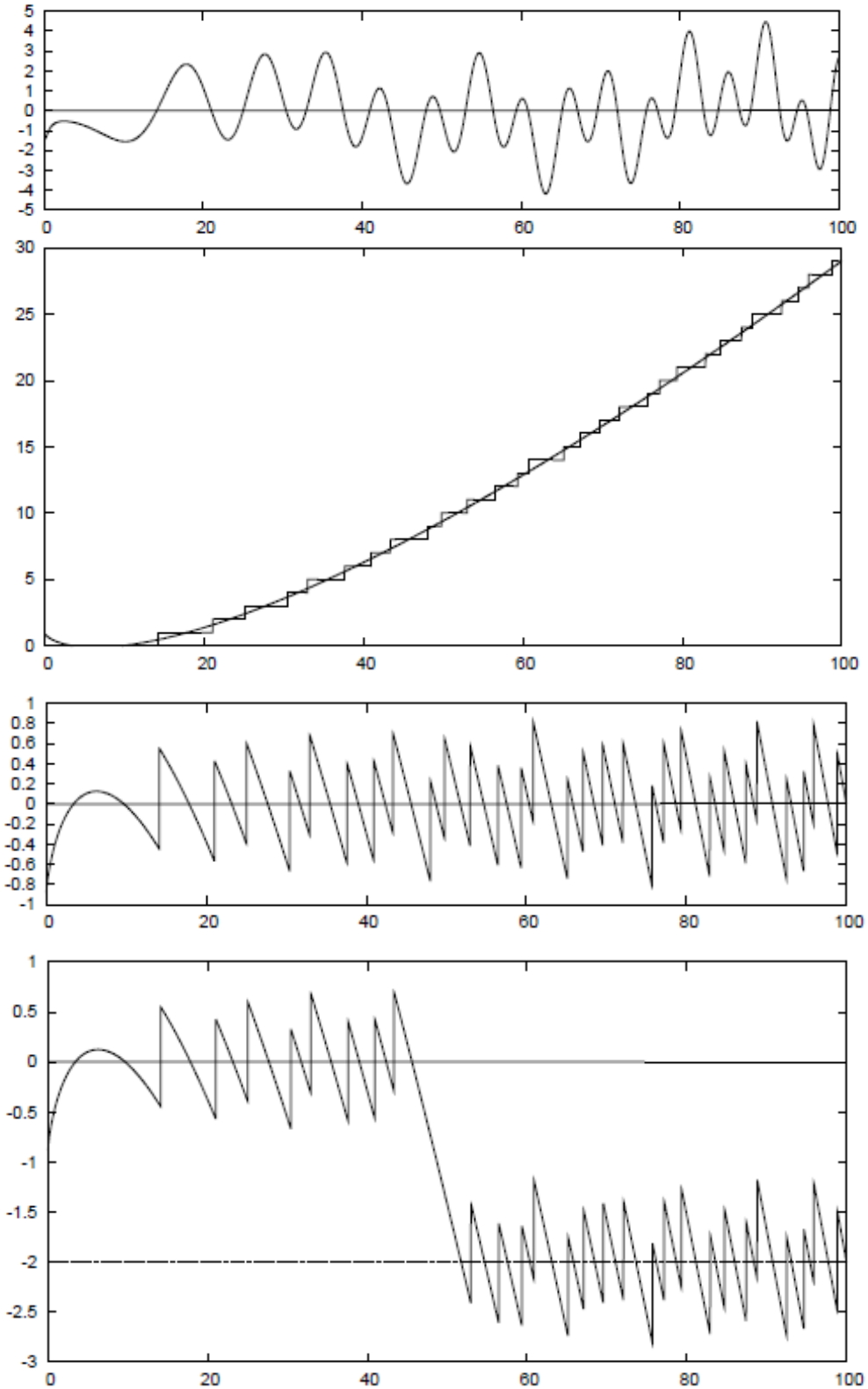

FIGURE 2. De haut en bas : $Z(t), N(T)$ vs. $M(T), E(T)$, et $E(T)$ avec une paire de zéros "manquant"

(La Figure 2, seconde partie, montre les graphes de $N(T)$ et $M(T)$ pour T allant jusqu'à 100. Remarquons comment chaque saut dans le graphe de $N(T)$ a lieu lorsque $Z(t)$ s'annule ; cela confirme

HR jusqu'à 100). Ceci est une approximation asymptotique, ce qui signifie que le pourcentage d'erreur de la prédiction tend vers 0 lorsque T croît, mais en termes absolus cela peut être faux dans une grande proportion pour une valeur de T particulière. En pratique, on n'a jamais observé d'erreur supérieure à 4, bien que l'on sache que l'erreur est particulièrement élevée pour de grandes valeurs de T. Dans tous les cas, cela rend la formule inutilisable quand on vient à prendre la décision de savoir si on a trouvé tous les zéros pour une valeur donnée de T.

Turing a eu l'intelligente idée de regarder le terme d'erreur $E(T) = N(T)–M(T)$ pour un domaine de valeurs de T plutôt que pour une seule. Littlewood a démontré que $E(T)$ a une valeur moyenne proche de 0 quand T est grand, et alors, il tend à osciller autour de 0, comme cela est visible dans la Figure 2, troisième partie. Si on imagine dessiner ce graphe en utilisant les données mesurées, tous les zéros qui ont été oubliés devrait biaiser la moyenne ; par exemple, si on oubliait deux zéros [17], cela devrait commencer à osciller aux alentours de -2, comme on le voit dans la partie basse de la figure. On peut transformer cela en une preuve rigoureuse qu'aucun zéro ne manque, dès qu'on dispose d'une version du théorème de Littlewood avec des constantes explicites. L'un des résultats théoriques principaux dans l'article de Turing [11] était une dérivation minutieuse d'un tel théorème.

Bien que Turing ait mené ses recherches en 1950, son article n'a pas été publié jusqu'en 1953, juste un an avant sa mort. Le projet n'était apparemment pas une priorité pour le Mark 1, comme on l'entend clairement dans la citation suivante de l'article [18] :

> Les calculs avaient été planifiés quelques temps à l'avance, mais ils durent être menés en toute hâte. Si ça n'avait pas été à cause du fait que l'ordinateur resta en service durant une période anormalement longue de 3 heures de l'après-midi, à 8 heures le lendemain matin, il est probable que les calculs n'auraient jamais été effectués du tout. Comme c'était le cas, l'intervalle $2\pi.63^2 < t < 2\pi.64^2$ fut étudié pendant cette période, et peu de choses supplémentaires furent faites.

Évidemment, Turing était déçu des résultats obtenus. Comme on le sait maintenant, les ordinateurs sont devenus beaucoup plus rapides, moins chers, et plus fiables qu'en 1950, et ces améliorations vinrent très vite. Pourtant, il aurait été difficile d'anticiper à ce moment-là, ce qui pourrait expliquer le pessimisme de Turing. D. H. Lehmer doit dire cela dans la Revue mathématique de l'article :

> Bien que l'auteur tende à rabaisser les résultats effectifs obtenus en quelques heures de temps machine, l'article montre qu'une grande quantité de travail minutieux a été menée pour préparer le calcul de la machine, et ce travail sera d'une grande valeur pour les futurs ordinateurs. Depuis 1950, il y a eu une grande augmentation du nombre et de la fiabilité des ordinateurs à grande échelle. Il ne fait pas de doute que des résultats ultérieurs au sujet de ce problème apparaîtront en temps utile.

En effet, vers 1956, Lehmer lui-même avait appliqué la méthode de Turing pour étendre les calculs à des domaines bien au-delà de la limite des calculateurs mécaniques. Avec des ordinateurs modernes

17. Puisque les zéros sont localisés par les changement de signes, on en rate toujours un nombre pair.

18. Le Mark 1, comme tous les premiers ordinateurs digitaux électroniques, utilisait des milliers de *tubes à vide* (ou valves thermiques), une technologie qui a évolué depuis les anciennes ampoules lumineuses incandescentes. Comme c'est le cas avec les ampoules lumineuses, on peut s'attendre à ce qu'un unique tube dure des années, mais lorsqu'on utilise des milliers d'entre eux, il était inévitable que l'un au moins tombe en panne chaque jour. Pour se prémunir de cela, c'était une pratique courante sur le Mark 1 que de répéter des sections de code toutes les quelques minutes et d'arrêter la machine quand une discordance était observée.

et des algorithmes améliorés, ils ont atteint des limites qui auraient été insondables dans les années 1950. Par exemple, il a été montré que les 10 trillions de premiers zéros vérifient HR, comme le fait également le $1032^{\text{ième}}$ zéro et des centaines de ses voisins ; tous ses calculs continuent de reposer sur la méthode de Turing comme petit élément essentiel. Il est malheureux que Turing n'ait jamais vu aucun de ces événements advenir.

Preuves formelles. Il y a de nombreuses autres citations intéressantes dans l'article de Turing de 1953 [11], mais l'une d'elles en particulier indique son état d'esprit d'alors [19] :

> Si des règles définitives sont fournies sur la manière dont le calcul doit être effectué, on peut prédire les limites pour les erreurs. Quand les calculs sont faits à la main, il y a de sérieuses difficultés pratiques à ce propos. Le calculateur aura sûrement ses propres idées sur la manière dont certaines étapes doivent être effectuées. [...] Pourtant, si les calculs sont faits par un ordinateur, on peut être sûr que cette sorte d'indiscipline n'aura pas lieu.

On peut noter que Turing était en train d'écrire "Machines calculatrices et intelligence" environ au même moment, et dans ce contexte, la citation n'est pas surprenante. Pourtant, c'était bien en avance sur le temps d'alors ; même deux décades plus tard, quand la première preuve du *théorème des quatre couleurs* fut annoncée, il y avait de sérieux doutes sur le fait qu'elle puisse être acceptée s'il n'était pas possible qu'un humain ne la vérifie. Turing déclarait en 1950 que non seulement cette preuve était acceptable mais qu'en fait, il était *préférable* que des machines remplacent des humains dans certains contextes.

Le vent est lentement en train de tourner en faveur du point de vue de Turing, dans le sens où certains mathématiciens font aujourd'hui davantage confiance à des résultats obtenus par ordinateur, bien qu'on entende fréquemment l'argument que de telles preuves sont moins élégantes que celles obtenues par "pensée pure". Le décalage dans les perceptions est illustré par une autre controverse, semblable à celle qui entoure le théorème des quatre couleurs, concernant la preuve de Thomas Hales en 1998 de la *conjecture de Kepler* ; en ce temps-là, ce n'était pas tant le problème de savoir s'il était possible de faire confiance à l'*ordinateur* mais ses programmeurs, puisque l'implémentation était techniquement un tel défi.

Comme l'utilisation des ordinateurs en mathématiques pures augmente, et comme les preuves deviennent plus compliquées de ce fait, de telles controverses semblent plutôt devenir plus fréquentes. Une réponse à cela est l'intérêt florissant pour les *preuves formelles* [6], dans lesquelles un ordinateur est utilisé pour vérifier chaque étape en commençant par les axiomes de base ; par exemple, on a maintenant deux preuves formelles indépendantes du théorème des nombres premiers, toutes deux achevées dans la dernière décennie. En suivant cette mode, il est facile d'imaginer un futur dans lequel la vision de Turing est de facto standard, et les preuves mathématiques ne devraient pas être acceptées tant qu'elles n'ont pas subi une vérification formelle par une machine.

19. L'utilisation par Turing du mot "calculateur" ici pour faire référence à un humain témoigne de l'usage courant jusqu'aux années 1940.

Étant données les économies d'échelles obtenues en terme de vitesse, fiabilité, et disponibilité des calculateurs notées ci-dessus, il n'est pas surprenant que leur utilisation ait explosé dans toutes sortes de tâches nécessitant des efforts humains. Par exemple, pour en revenir aux tests de primalité, c'est devenu une tâche ordinaire que de trouver des nombres premiers avec des milliers de chiffres, et cela permet de préserver la sécurité des transactions en ligne.

Pour la théorie analytique des nombres et HR en particulier, une grande quantité de nouvelles compréhensions ont été obtenues à partir des calculs de la fonction zeta, essentiellement dans l'esprit du travail de Turing en 1950. Avant toute chose, parmi elles, il y a les calculs effectués dans les années 1980 par Andrew Odlyzko qui, avec Schönhage, a trouvé un algorithme qui pouvait calculer plusieurs valeurs de $Z(t)$ simultanément très rapidement, ce qui fut la première amélioration théorique selon ces lignes depuis la découverte de la formule de Riemann-Siegel. Le nouvel algorithme permit à Odlyzko de montrer un lien entre les zéros de la fonction zeta et la *théorie des matrices aléatoires*, un outil utilisé par les physiciens pour modéliser les niveaux d'énergie des atomes lourds. La figure 3 montre un graphe produit par Odlyzko et comparant la distribution de l'espacement entre plus proches voisins des zéros de la fonction zeta à celle des valeurs propres de matrices hermitiennes aléatoires (cet ensemble appelé l'*ensemble GUE*). Pour le dire grossièrement, la courbe donne la probabilité qu'un saut d'une taille donnée advienne entre deux zéros consécutifs ; ainsi, par exemple, on voit que les zéros sont rarement proches les uns des autres, i.e. ils ont tendance à se repousser les uns les autres.

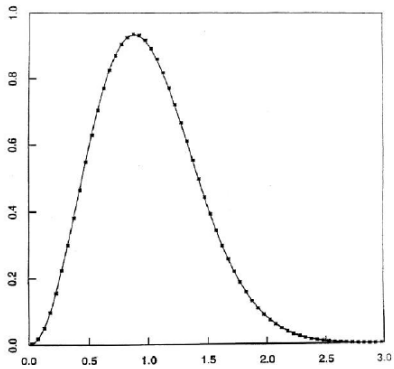

Figure 3. Distribution de l'espacement au plus proche voisin d'environ 79 millions de zéros autour du $1020^{\text{ième}}$ zéro (nuage de points), comparé avec le modèle GUE (courbe lisse).

Le premier soupçon d'une connexion entre la fonction zeta et la théorie des matrices aléatoires est venu d'une heureuse rencontre entre le mathématicien Hugh Montgomery et le physicien Freeman Dyson à l'Institut des études avancées en 1972. Montgomery avait conjecturé une formule pour une valeur statistique, la *corrélation de paires* des zéros de la fonction zeta, et Dyson reconnut immédiatement que la formule était identique à celle du modèle GUE. Pourtant, les résultats numériques d'Odlyzko, comme on le voit dans la figure 3, furent décisifs pour la défense des arguments en faveur d'une idée qui aurait pu sembler n'être qu'une curieuse coïncidence.

Ce qui reste confus, c'est la *raison* pour laquelle les zéros de la fonction zeta suivent les statistiques GUE. Une possibilité est qu'il y a un système physique, similaire à un atome lourd, dont le spectre

est exactement l'ensemble des zéros de ζ. S'il en était ainsi, trouver le système rendrait effective une approche, qu'on appelle de nos jours la conjecture de Hilbert-Pólya pour prouver HR et qui avait été suggérée par Pólya il y a un siècle.

Une possibilité plus banale est que ce phénomène soit universel, de la même façon que les distributions gaussiennes s'avèrent nombreuses dans la nature, une vision renforcée par des calculs faisant intervenir d'autres L-fonctions qui ont trouvé des résultats similaires. Il y a maintenant de nombreux objets mathématiques que l'on appelle du nom général de L-fonction [1], et dont les prototypes sont la fonction zeta de Riemann et les L-fonctions originales de Dirichlet. Le *programme de Langlands*, un domaine majeur de recherches en théorie moderne des nombres, vise à classifier les différentes sortes de fonctions et les relations entre elles, et l'on commence tout juste à explorer le potentiel complet des méthodes computationnelles dans ce domaine [20]. En partie, l'intérêt pour les autres L-fonctions a grandi de notre incapacité à démontrer HR, puisque quand les mathématiciens sont coincés sur un problème, ils essaient souvent de faire des progrès dans différentes directions en généralisant. Ainsi, chacune de ces L-fonctions plus générales a une "hypothèse de Riemann associée", bien qu'il n'y ait toujours pas de cas pour lequel une telle hypothèse ait été prouvée.

Quelle que soit la raison du phénomène GUE, on peut arguer qu'une compréhension complète de celui-ci est nécessaire avant qu'une preuve de HR ne puisse être trouvée. Bien que ceci semble encore nécessiter un long chemin avant que le but ne soit atteint, nous en sommes juste actuellement au point de vérifier des conjectures, comme Turing et Odlyzko l'ont fait, et nous commençons à utiliser de tels calculs comme remplacement de HR quand nous résolvons des problèmes. Voici trois exemples liés aux nombres premiers :

(1) *Compter les nombres premiers.* Comme on l'a vu, la formule de Gauss donne une bonne approximation du nombre de nombres premiers qu'il y a parmi les nombres 2, 3, ..., x . Mais qu'en est-il si l'on souhaite connaître le nombre exact de nombres premiers inférieurs à x pour un x donné ? Jusqu'au $19^{\text{ième}}$ siècle, le meilleur moyen de déterminer cela était de trouver tous les nombres premiers par le crible d'Ératosthène et de les compter. Heureusement, les mathématiciens ont trouvé quelques méthodes plus intelligentes depuis ce temps. La méthode la plus rapide récemment découverte est celle proposée par Lagarias et Odlyzko en 1987 ; elle fonctionne en ajoutant différents termes d'erreur à la formule de Gauss en utilisant les calculs qui interviennent dans la vérification de HR. Une version de cette méthode a été utilisée pour la première fois en 2010 par Buethe, Franke, Jost et Kleinjung, qui ont calculé la dernière entrée de la table 2. Leur méthode suppose HR vraie, mais cette supposition a très récemment été supprimée dans un calcul indépendant par Platt.

(2) *Le problème* $\pi(x)$ *vs.* $\mathrm{Li}(x)$. En utilisant des approximations numériques des 22 millions premiers zéros de la fonction zeta de Riemann, Saouter et Demichel ont montré en 2010 que $\pi(x)$ excède $\mathrm{Li}(x)$ pour une certaine valeur de x en-dessous de 1.3972×10^{316}, et il y a des raisons de croire que la première occurrence est proche de ce nombre. Ainsi, alors qu'il se peut qu'on ne connaisse jamais la première occurrence exactement, la question de la meilleure approximation possible de la limite de Skewes a effectivement été résolue.

(3) *La conjecture de Goldbach.* Le 7 juin 1742, Christian Goldbach a écrit une lettre à Euler

20. Voir (dans l'article initial, il est fait référence au site www.L-functions.org qui n'existe plus et est remplacé, du moins le croyons-nous, par) www.lmfdb.org.

dans laquelle il a conjecturé que tout entier supérieur à 5 peut s'écrire comme la somme de trois nombres premiers [21]. Aucun progrès essentiel n'a été fait sur cette conjecture jusqu'au $20^{\text{ième}}$ siècle. Dans les années 1930, Vinogradov a montré que la conjecture est vraie pour tous les nombres *impairs* suffisamment grands, bien que le cas pair reste insaisissable. (La conjecture s'avère beaucoup plus difficile pour les nombres pairs, puisqu'au moins l'un des trois nombres premiers doit être 2 dans ce cas, ne laissant seulement que deux degrés de liberté.) Ici la signification de "suffisamment grand" a été réduite au cours des ans, mais elle reste encore au-dessus de 10^{1300}, un nombre beaucoup trop grand pour tester tous les nombres plus petits que lui directement, même avec les ordinateurs modernes. D'un autre côté, on sait que la conjecture de Goldbach est vraie pour les nombres impairs si HR est vraie pour la fonction zeta de Riemann et pour les L-fonctions de Dirichlet. La vérification numérique de HR, comme dans le travail de Turing promet de nous permettre de franchir l'écart entre ces résultats dans un futur pas si lointain.

En plus d'effectuer des recherches sur les conjectures et les problèmes existant, les 60 dernières années se sont avérées extrêmement utiles pour suggérer de nouvelles lignes d'approche. Un bon exemple est la *conjecture BSD*, découverte au début des années 1960 par Birch et Swinnerton-Dyer en utilisant le EDSAC à Cambridge. La conjecture concerne *les courbes elliptiques*, qui sont des équations de la forme $y^2 = x^3 + ax + b$, où a et b sont des entiers fixés. (Les courbes elliptiques sont le sujet d'un autre problème célèbre en théorie des nombres, la conjecture de Shimura Taniyama, dont la preuve par Wiles et Taylor en 1995 a finalement amené à une preuve complète du dernier théorème de Fermat après 350 ans d'efforts.) Étant donnée une courbe elliptique, on peut lui associer une L-fonction, et comme l'hypothèse de Riemann avant elle, la conjecture BSD est une prédiction à propos des zéros de cette fonction. On considère maintenant ce problème comme étant l'un des plus importants problèmes ouverts de la théorie des nombres, et même des résultats partiels dans sa direction ont eu des applications étonnantes. L'une d'entre elles est la résolution par Tunnell en 1983 du problème âgé de 1000 ans dit *problème des nombres congruents* [2], qui demande s'il existe, pour un nombre donné n, un triangle rectangle qui a comme aire n et dont les longueurs des côtés sont des nombres entiers. (Stricto sensu, on peut seulement prouver que l'algorithme de Tunnell fonctionne en supposant la conjecture BSD, mais une preuve complète de la conjecture n'est pas nécessaire pour appliquer l'algorithme). Un autre exemple est la résolution effective de Goldfeld du *problème du nombre de classes* [5], posé par Gauss en 1801 ; par exemple, son travail nous explique (entre de multiples autres choses) que tous les entiers peuvent s'écrire de manière unique comme une somme de trois carrés parfaits.

Ainsi, les ordinateurs ont été instrumentalisés pour le traitement de problèmes restés non résolus pendant longtemps (parfois même des problèmes anciens) en théorie des nombres. D'un autre côté, il y a d'autres questions pour lesquelles nos techniques courantes semblent totalement inadaptées pour les résoudre, ce qui laisse les expérimentations numériques comme étant la seule manière de les attaquer à présent. Par exemple, on a déjà rencontré quelques-unes de telles questions dans ce chapitre, questions pour lesquelles notre connaissance théorique n'est significativement pas plus avancée que celle d'Euclide en 300 avant J.-C. environ :

21. Il était encore courant de considérer 1 comme un nombre premier au temps de Goldbach, et donc il a effectivement écrit 2 à la place de 5.

(1) Est-ce que tout nombre premier apparaît dans la première séquence d'Euclide-Mullin ?
(2) Y a-t-il des nombres parfaits impairs ?
(3) Y a-t-il un nombre infini de nombres premiers de Mersenne ?

On ne devrait jamais tenter de placer une limite à l'ingéniosité des êtres humains (ou de leurs machines), mais comme Gödel l'a montré, il y a des questions pour lesquelles on ne peut connaître la réponse, et il est concevable que l'une d'entre elles soit dans cette catégorie. (En fait, trouver un exemple "naturel" d'une telle question était la motivation originale derrière la construction de Mullin). D'une certaine manière, cela est bon, puisque ça laisse ouverte une avenue pour les mathématiciens amateurs et dont c'est le hobby, y compris ceux qui peuvent former la prochaine génération des théoriciens des nombres informaticiens, pour s'impliquer dans ce qui deviendrait sinon un sujet sophistiqué et impénétrable.

Le futur des ordinateurs en théorie des nombres. Nous voici arrivés à une époque maintenant où presque tout mathématicien a sur son bureau un outil auquel Gauss ne pouvait que rêver. Comme on l'a vu ci-dessus, les ordinateurs commencent à façonner les résultats en théorie des nombres. Il semble que cette tendance continuera jusqu'à ce que les ordinateurs soient devenus indispensables pour faire de la recherche, et où personne ne travaillera complètement sans eux. Peut-être, comme une évolution naturelle du boom actuel sur les preuves formelles, les ordinateurs finiront par faire quelques raisonnements par eux-mêmes.

Dans un exposé célèbre en 1900, David Hilbert a donné une liste de 23 problèmes non résolus décrivant sa vision du développement des mathématiques dans le prochain siècle. Le problème numéro 8 de la liste était la théorie des nombres, incluant à la fois HR et la conjecture de Goldbach. Malheureusement, nous ne sommes guère plus proches d'une preuve d'HR aujourd'hui qu'en 1900, avec des découvertes telles qu'un lien avec la théorie des matrices aléatoires qui semble engendrer plus de questions que de réponses. (Hilbert aurait pu anticiper cela ; il l'énonce dans cette citation "Si je me réveillais après avoir dormi un millier d'années, ma première question serait : l'hypothèse de Riemann a-t-elle été résolue ?"). Néanmoins, un progrès significatif a été fait sur la plupart des problèmes de Hilbert, quelquefois de manières inattendues ; par exemple, le travail de Gödel mentionné ci-dessus, ainsi que celui de Turing après lui, était très contraires aux attentes de Hilbert.

Au tournant d'un nouveau siècle en 2000, plusieurs listes furent proposées en remplacement de celle des problèmes de Hilbert. Celle qui a reçu le plus d'attention est la liste des sept problèmes du millénaire publiée par l'Institut Clay des mathématiques, qui offre un million de dollars pour la solution d'un quelconque d'entre eux. Jusque-là, un problème, la conjecture de Poincaré, a été résolu. Des six problèmes restant, nous en avons rencontré trois dans ce chapitre au sujet du travail de Turing : l'hypothèse de Riemann, la conjecture BSD et le problème P vs. NP. Cela ne signifie pas que les recherches de Turing sur le Manchester Mark 1 aient eu une grande influence directe sur ces choses, mais au moins, cela témoigne de l'étrange capacité de Turing à reconnaître et à s'impliquer dans des problèmes d'intérêt durable.

À quoi ressemblera la liste des problèmes du $22^{\text{ième}}$ siècle ? Il est probable qu'aucune personne vivante aujourd'hui ne puisse faire une prédiction significative. Pourtant, il semble sain de parier

qu'une telle liste contiendra au moins un problème de théorie des nombres ; si tel est le cas, peut-être sera-ce l'un des problèmes qui a été découvert par un ordinateur. Turing, qui n'avait jamais peur de donner son sentiment, l'a mieux dit dans une interview après la couverture de presse initiale pour le Mark 1 :

> C'est seulement un avant-goût de ce qui va advenir, et seulement l'ombre de ce qui sera. Nous devons avoir quelque expérience avec la machine avant de connaître ses capacités. Cela peut prendre des années avant que les nouvelles possibilités ne soient installées, mais je ne vois pas pourquoi ces possibilités ne pourraient pas être utilisées dans n'importe lequel des domaines normalement couvert par l'intelligence humaine et finalement, rivaliser sur un pied d'égalité.

Références

[1] Andrew R. Booker. Uncovering a new L-function. *Notices Amer. Math. Soc.*, 55(9) : 1088-1094, 2008.

[2] V. Chandrasekar. The congruent number problem. *Resonance*, 3 : 33-45, 1998. 10.1007/BF02837344.

[3] J. Brian Conrey. The Riemann Hypothesis. *Notices Amer. Math. Soc.*, 50(3) : 341–353, 2003.

[4] Leo Corry. Hunting prime numbers from human to electronic computers. *Rutherford Jour.*, 3, 2010.

[5] Dorian Goldfeld. Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. (N.S.)*, 13(1) : 23-37, 1985.

[6] Thomas C. Hales. Formal proof. *Notices Amer. Math. Soc.*, 55(11) : 1370–1380, 2008.

[7] Dennis A. Hejhal. A few comments about Turing's method. Dans S. Barry Cooper et J. van Leeuwen éditeurs, *Alan Turing His Work and Impact.* Elsevier Science, 2012.

[8] Dennis A. Hejhal and Andrew M. Odlyzko. Alan Turing and the Riemann zeta function. Dans S. Barry Cooper et J. van Leeuwen éditeurs, *Alan Turing His Work and Impact.* Elsevier Science, 2012.

[9] Andrew Hodges. *Alan Turing : the enigma.* Un livre Touchstone. Simon et Schuster, New York, 1983. Les chapitres 6 et 7 couvrent la période dont il est question ici, incluant une histoire détaillée de la conception et du développement des ordinateurs ACE et Manchester Mark 1.

[10] Władysław Narkiewicz. *The development of prime number theory : From Euclid to Hardy and Littlewood.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

[11] A. M. Turing. Some calculations of the Riemann zeta-function. *Proc. London Math. Soc.* (3), 3 : 99-117, 1953.

[12] D. Zagier. Newman's short proof of the prime number theorem. *Amer. Math. Monthly*, 104(8) : 705-708, 1997.