Revue d'histoire des mathématiques,
4 (1998), p. 191–236.

L'ARITHMÉTICIEN ÉDOUARD LUCAS (1842–1891) : THÉORIE ET INSTRUMENTATION

Anne-Marie Décaillot (*)

Résumé. — Édouard Lucas est étudié, dans l'article qui suit, comme une des figures les plus représentatives du milieu des arithméticiens français de la seconde moitié du XIX^e siècle, milieu à qui on doit notamment des méthodes de calcul rapides et des algorithmes. À travers les éléments biographiques présentés dans la première partie, le caractère marginal de Lucas (et corrélativement de tout ce milieu) est mis en évidence. La nature des problèmes abordés par Lucas, les lieux d'expression et de publication de ses résultats et ses difficultés de carrière en témoignent. La deuxième partie de l'article est consacrée à l'examen des principaux résultats théoriques de Lucas : petit théorème de Fermat et tests de primalité. La conception d'un instrument arithmétique destiné à tester mécaniquement la primalité de certains grands nombres entiers est au centre de la troisième partie. La postérité des travaux de Lucas, plus importante à l'étranger, et notamment aux États-Unis, qu'en France, est abordée en fin d'article.

Abstract. — Édouard Lucas (1842–1891), the arithmetician : theory and instrumentation. — In this article, Edouard Lucas is studied as one of the most representative figures of the French arithmeticians' milieu, which was responsible for fast computing methods and algorithms in the second half of the 19th century. Some biographical elements presented in the first part show that Lucas (and correlatively this whole milieu) exhibited marginal aspects, as witnessed by the nature of the problems tackled by Lucas, his results' outlets for publication, and his career difficulties. The second part of this paper is devoted to the examination of Lucas's principal theoretical results : Fermat's "little" theorem and primality tests. The conception of an arithmetical instrument designed for testing the primality of certain large numbers is the focus of the third part. More important abroad (and notably in the United States) than in France, the posterity of Lucas's work is touched upon at the end of the article.

L'arithméticien Édouard Lucas (1842-1891) apparaît comme l'un des auteurs français les plus prolifiques de la fin du XIX^e siècle dans le domaine de la théorie des nombres. Lucas se rattache au groupe de

(*) Texte reçu le 15 décembre 1997, révisé le 4 février 1999.
Anne-Marie Décaillot, UFR de Mathématiques et Informatique, Paris V, 45 rue des Saints Pères, 75006 Paris et Groupe d'histoire et de diffusion des sciences d'Orsay.
Courrier électronique : deca@math-info.univ-paris5.fr.

mathématiciens français se référant à une tradition algébrique classique de la discipline. Il est également connu pour ses œuvres de vulgarisation, récréations mathématiques et arithmétique amusante. Prédominante entre 1870 et 1900, cette catégorie d'arithméticiens disparaît presque entièrement des publications académiques françaises au début du XX^{e} siècle ; le renouveau disciplinaire met alors en avant la théorie des formes et la théorie analytique des nombres. À travers le personnage de Lucas, c'est une meilleure connaissance de ce groupe qui est visée. Marginaux par rapport au milieu académique et universitaire, publiant dans des revues considérées de second plan, travaillant sur des questions négligées par les autres mathématiciens de l'époque (calcul algorithmique et calcul mécanique en arithmétique par exemple), ces scientifiques connaissent aujourd'hui un fort regain d'intérêt. Il faut souligner que Lucas est un membre actif d'une société savante, la Société Mathématique de France (SMF), et d'une association à caractère scientifique, l'Association Française pour l'Avancement des Sciences (AFAS).

Tombée en France dans un oubli relatif au début du XX^{e} siècle[1], l'œuvre de Lucas est enrichie par les Anglo-Saxons, en particulier par Derrick Henry Lehmer dans les années 1930. Elle ressort aujourd'hui de l'indifférence, la cryptographie remettant à l'honneur la recherche de très grands nombres premiers[2]. Les plus grands d'entre eux découverts dernièrement sont des nombres de Mersenne, c'est-à-dire de la forme 2^n-1, et le critère de primalité utilisé demeure celui de Lucas-Lehmer. L'intérêt de la contribution de Lucas à l'étude des questions de primalité, au moyen de tests puissants et rapides, s'en trouve justifié.

La première partie de l'étude qui suit est consacrée à ces arithméticiens français de la deuxième moitié du XIX^{e} siècle et à quelques éléments de la biographie de Lucas. À travers la carrière parfois difficile de ce scientifique, nous nous efforçons de montrer le caractère marginal de ce groupe par rapport au milieu mathématique français classique. Dans la deuxième partie, nous nous intéressons à l'apport théorique de Lucas concernant le petit théorème de Fermat et le domaine des tests de primalité. Le principe

[1] Eugène Cahen est chargé d'un cours de théorie des nombres à la Sorbonne entre 1910 et 1915. Il publie en 1900 des *Éléments de théorie des nombres* [Cahen 1900], ouvrage pour une large part algébrique, dans lequel il omet de faire référence à Lucas et à son traité de *Théorie des nombres* [Lucas 1891], qui ne date pourtant que de 1891.

[2] Voir, par exemple, le *Cours d'algèbre* de Michel Demazure [1997].

de l'instrument arithmétique, que Lucas qualifie de mécanisme et parfois de «*machine arithmétique*», destiné à tester la primalité de certains grands nombres entiers, est analysé dans la troisième partie. Cette machine a-t-elle été construite en 1891 par l'ingénieur civil Henri Genaille, sous le nom de piano arithmétique, comme certains témoignages le laissent à croire ? Ce dernier s'est-il contenté d'en dessiner les plans ? La question demeure posée. L'analyse de la postérité de Lucas constitue la dernière partie. L'influence de l'arithméticien est beaucoup plus faible en France, où le calcul numérique et algorithmique rapide est longtemps négligé[3], qu'à l'étranger, essentiellement aux États-Unis.

ÉDOUARD LUCAS, FIGURE REPRÉSENTATIVE DU MILIEU DES ARITHMÉTICIENS FRANÇAIS DE LA DEUXIÈME MOITIÉ DU XIX^{e} SIÈCLE

À l'exception de Charles Hermite, la théorie des nombres préoccupe assez peu le milieu mathématique français classique avant 1910. On peut remarquer qu'elle est absente de l'enseignement supérieur (facultés des sciences et grandes écoles). Contrairement aux universités étrangères, il n'existe aucune chaire de théorie des nombres dans l'Université française, hormis la charge de cours d'Eugène Cahen entre 1910 et 1915 à la Sorbonne. La tradition allemande est plus ancienne et les universités germaniques sont au cœur de l'enseignement et de la recherche en ce domaine : ainsi Ernst Eduard Kummer est nommé professeur à Breslau en 1842, puis à Berlin ; parmi ses élèves figurent Leopold Kronecker et Paul Bachmann, qui occupent à leur tour des fonctions universitaires. Les notes des cours de théorie des nombres de Gustav Lejeune-Dirichlet et Richard Dedekind, *Vorlesungen über die Zahlentheorie*, paraissent en 1863[4].

En France, le milieu des théoriciens des nombres est constitué pour l'essentiel de professeurs de l'enseignement secondaire et de membres d'associations à caractère scientifique, comme l'AFAS. Ces arithméticiens s'expriment dans des notes aux *Comptes rendus* de l'Académie des sciences (CRAS), dont l'analyse est faite de 1870 à 1914 par Catherine Goldstein [1994]. Lucas apparaît comme l'un des auteurs les plus féconds en

[3] Voir [Tournès 1998].

[4] Voir Catherine Goldstein, *Le métier des nombres*, dans [Serres 1989, p. 275–295].

ce domaine (neuf notes pendant la période considérée). Il appartient au groupe de mathématiciens français intéressés par les aspects algébriques traditionnels de cette discipline, dont les références vont de Fermat, des Bernoulli, d'Euler, de Lagrange et de Legendre aux *Disquisitiones* de Gauss. Leurs études (environ 130 notes aux CRAS) portent pour l'essentiel sur les nombres premiers, les diviseurs d'un nombre donné, les fractions continues, l'analyse diophantienne, les équations à coefficients entiers. Cette catégorie d'arithméticiens est prédominante entre 1870 et 1900. Elle disparaît presque entièrement des notes aux *Comptes rendus* au début du XX^{e} siècle, au moment où se manifestent un renouveau thématique, ainsi que des changements de perspective et de niveau d'exigence de la discipline. L'explosion de nouvelles recherches met alors en avant la théorie analytique des nombres et la théorie des formes ; celle des corps de nombres émerge.

Hélène Gispert analyse les recherches françaises de haut niveau, notamment les thèses soutenues entre 1870 et 1914 par des sociétaires de la Société Mathématique de France : la théorie des formes et la théorie des nombres y sont singulièrement peu présentes[5]. Pendant cette période le *Bulletin de la Société Mathématique de France* comporte seulement 6 % de communications en théorie des nombres contre 32 % en géométrie et 27 % en analyse[6]. Hormis les notes aux *Comptes rendus*, qui constituent de véritables publications de recherche, on peut s'interroger sur les lieux d'expression des résultats numériques français. Un élément de réponse est apporté par H. Gispert : «*Ces disciplines semblent être principalement cultivées dans le cadre de revues de diffusion ou d'enseignement*» qui proposent en guise de récréations mathématiques des questions de théorie des nombres, d'analyse diophantienne ou de divisibilité par exemple. Le recensement effectué par Leonard Eugene Dickson et ses collaborateurs confirme par ailleurs le rôle de la revue française *Nouvelles annales de mathématiques*, ainsi que des revues belges *Nouvelle correspondance*

[5] Parmi les thèses soutenues à la faculté des sciences de Paris, on peut mentionner celle du R.P. Joubert (août 1876) sur l'application des fonctions elliptiques à l'arithmétique supérieure, et celle de Léon Charve (juillet 1880) sur l'application de la théorie arithmétique à un nouveau mode d'approximation contenant les fractions continues (dont le rapport, rédigé par Ch. Hermite, est conservé aux Archives nationales (désormais A.N.) AJ^{16} 5533).

[6] Voir [Gispert 1991, p. 86, 91, 158 et tableau p. 173].

mathématique et *Mathesis* dans le domaine numérique[7].

Dans l'édition, les années 1880–1900 sont marquées en France par un besoin de mise à jour des connaissances mathématiques : de grands traités paraissent où l'analyse est la préoccupation dominante. Or en algèbre et en théorie des nombres les traités sont rares ; dans ce paysage, l'ouvrage *Théorie des nombres* d'Édouard Lucas, publié en 1891, fait exception. Il sera suivi du traité remarquable constitué des conférences de Jules Tannery à l'École normale supérieure, rédigées par Émile Borel pour l'algèbre et Jules Drach pour la théorie des nombres, ainsi que du traité d'Eugène Cahen[8]. Ces efforts sont insuffisants pour assurer la présence française lors du congrès international de mathématiques qui se tient à Zürich en 1897, où la section d'algèbre et de théorie des nombres ne comporte aucun intervenant français.

Le désintérêt relatif du milieu académique français permet d'appréhender l'investissement d'un certain nombre de mathématiciens, par ailleurs membres de la SMF, très présents à l'AFAS dans le domaine arithmétique. Entre 1872 (année de la fondation de l'association) et 1914, les 1200 interventions de la section 1 du groupe des sciences mathématiques comportent 20 % de communications concernant des problèmes numériques. L'AFAS s'affirme ainsi comme un lieu d'expression et de publication de résultats concernant les nombres, au même titre que les revues de diffusion et d'enseignement. L'activité des arithméticiens y atteint une ampleur comparable à celle qui se déploie au travers des notes aux *Comptes rendus*. Sans être des mathématiciens d'exception, ces scientifiques ont une action et une influence qui ne peuvent être tenues pour négligeables[9].

---

[7] Voir [Dickson 1919–1923].

[8] Voir [Tannery 1895] et [Cahen 1900].

[9] Parmi eux nous trouvons : Aubry, Fontès, Gérardin, Gohierre de Longchamps, Laisant, Lucas, Maillet, d'Ocagne, Pellet, Perrin. Pour sa part, Henri Poincaré effectue deux communications tout à fait exceptionnelles au congrès de l'association en 1881. L'une porte sur « *les invariants arithmétiques et leur utilisation pour reconnaître si deux formes quadratiques sont équivalentes* » [AFAS 1881, p. 109–117], l'autre sur « *les applications de la géométrie non euclidienne à la théorie des formes quadratiques* » [AFAS 1881, p. 132–138]. Il faut souligner à ce propos que des étrangers, et parmi eux des savants de tout premier plan comme Cantor, Peano, Sylvester ou Tchebychef, n'hésitent pas à utiliser l'AFAS pour diffuser certains de leurs résultats.

L'arithmétique pratiquée par ce milieu scientifique a trait aux problèmes de combinatoire appliquée, de calcul des probabilités, de jeux (dames, échecs, taquin en sont des exemples), de calendriers, à la construction de carrés magiques et à la diffusion de récréations mathématiques. Le souci du calcul mécanique et la présentation d'instruments pouvant le faciliter s'y rattachent, les intervenants à l'AFAS étant particulièrement représentatifs de ce courant. Un deuxième axe de préoccupations est constitué par des questions de divisibilité et de primalité des nombres. Les questions théoriques qui peuvent s'y rattacher sont exposées en général dans les notes aux *Comptes rendus* ou dans le *Bulletin* de la SMF, plus rarement à l'AFAS; la construction de tables très étendues de nombres premiers ou de diviseurs de nombres composés est réservée à l'association. Des tests de primalité, véritables algorithmes de calcul rapide valables pour de très grands nombres entiers, sont discutés entre auteurs de notes aux *Comptes rendus*, comme le R.P. Théophile Pépin, et intervenants à l'AFAS. L'arithmétique diophantienne, les équations de variables entières, les fractions continues constituent le troisième thème abordé par ces arithméticiens. Les travaux théoriques de leurs contemporains allemands, ou ceux d'Évariste Galois, sont peu utilisés ou méconnus; l'emploi de méthodes analytiques, l'utilisation de séries, quasi inexistants[10].

Le milieu académique français a peu de considération pour les travaux de ces arithméticiens, dont on réhabilite le rôle de nos jours[11]. Lucas apparaît comme le plus fécond, le plus intéressant d'entre eux. L'œuvre de Lucas (plus de 170 articles et 15 ouvrages d'importance diverse) est rédigée entre 1866, où paraît la première note au *Bulletin international de l'Observatoire de Paris*, et 1891, année de la mort de l'auteur, où est publié le premier volume de son traité de *Théorie des nombres*[12]. Nous ne

[10] En France, Jacques Hadamard contribue à l'émergence de ces méthodes analytiques. Il obtient le grand prix de l'Académie des sciences en 1892 pour sa réponse à la question de la «*détermination du nombre de nombres premiers inférieurs à une quantité donnée*» [Hadamard 1892], et publie en 1896 un mémoire «*Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques*» [Hadamard 1896]. On peut signaler également la thèse d'Eugène Cahen «*Sur la fonction $\zeta(s)$ et sur des fonctions analogues*», soutenue en mars 1894 devant Hermite, Picard et Poincaré.

[11] Des éléments d'appréciation de cette situation sont apportés par C. Goldstein dans [Serres 1987, p. 275–295].

[12] Pour une liste assez exhaustive des œuvres de Lucas voir la bibliographie de [Harkin 1957, p. 282–288]. On doit cependant la compléter par l'article du bulletin de

pouvons avoir l'ambition de rendre compte de toute son œuvre aux aspects multiples dans le cadre de cette étude. L'accent sera mis sur quelques résultats originaux qui lui sont dus dans le domaine de l'arithmétique aussi bien théorique qu'appliquée. Les éléments biographiques résultent d'une consultation de divers fonds d'archives nationales et départementales, des archives de l'École normale supérieure (ENS) et de l'Académie des sciences.

Un parcours difficile . . .

Les débuts d'Édouard Lucas sont ceux d'un enfant issu d'une famille de condition très modeste (son père est artisan tonnelier à Amiens). Une bourse communale lui permet d'accéder aux études secondaires et à la préparation aux concours des écoles spéciales de l'État. Il est reçu très honorablement en 1861 à l'École polytechnique et à l'École normale supérieure, en même temps que Gaston Darboux. Il opte pour cette dernière et, à sa sortie en 1864, il obtient le deuxième rang à l'agrégation de sciences mathématiques, la première place étant occupée par Darboux. Louis Pasteur, alors directeur des études scientifiques de l'ENS, apprécie «*la sagacité inventive dans certaines branches des mathématiques*» du jeune normalien[13]. La promotion « au mérite » d'un étudiant d'origine modeste, attiré par les sciences sous le Second Empire, mérite d'être soulignée. Quelques normaliens encouragés par Pasteur manifestent leur volonté de poursuivre dans la voie de la recherche scientifique : si le cas de Darboux demeure exemplaire, celui de Lucas n'en présente pas moins d'intérêt.

À la demande du directeur de l'Observatoire impérial de Paris, Urbain Le Verrier, Lucas est rattaché à cet établissement en septembre 1864, au titre d'astronome adjoint. La carrière de Lucas commence bien, Le Verrier considérant «*comme un devoir de laisser à l'Observatoire un corps de savants distingués*»[14]. Lucas demeure à l'Observatoire jusqu'à la fin de l'année 1869, ces cinq années étant marquées par les relations houleuses

l'Académie des sciences de Saint-Petersbourg [Lucas 1890]. Une erreur fait attribuer à Édouard Lucas une note aux *Comptes rendus* qui est en fait due à son homonyme Félix Lucas [CRAS 89, p. 224–226].

[13] Cité par [Combette 1892, p. 57–59]. Voir aussi les archives de l'ENS, A.N. AJ^{61} 38.

[14] Lettres de Le Verrier au ministre de l'Instruction publique et des cultes (10 et 14 septembre 1864), conservées dans le dossier administratif d'Édouard Lucas, A.N. F^{17} 22970.

des personnels de l'Observatoire avec leur directeur. Victor Puiseux[15] décrit la «*véritable atmosphère de guerre*» qui enveloppe l'établissement dans les années précédant 1870. La suppression des traitements de la plupart des adjoints et la demande par Le Verrier de leur destitution finit par émouvoir le ministre Victor Duruy, qui refuse ces décisions. Le goût des normaliens pour la recherche scientifique s'accommode mal des contraintes que le directeur de l'Observatoire fait peser sur ses collaborateurs et Édouard Lucas apparaît comme l'un des astronomes que Le Verrier cherche à évincer[16]. À la suite de ce conflit, Lucas quitte l'Observatoire de Paris. L'expérience acquise en tant qu'astronome adjoint peut expliquer son intérêt pour les procédures de calcul et la recherche d'instruments mécaniques permettant de les alléger. Cette pratique n'est guère encouragée au sein des observatoires d'astronomie, où le calcul à la main est encore seul pratiqué[17]. La longueur des calculs demandés au cours de la « réduction » des observations astronomiques (corrections nécessaires des phénomènes de réfraction) ou de l'établissement des trajectoires des corps célestes semble atteindre alors les limites des possibilités humaines. La révolte des astronomes peut y avoir puisé des raisons supplémentaires d'exaspération[18].

---

[15] Dans sa notice nécrologique de C. Wolf, *Annuaire de l'association des anciens élèves de l'École normale*, 1919, p. 8.

[16] Un *Mémoire sur l'état actuel de l'Observatoire Impérial*, Paris 1870, p. 16, signé de quatre chefs de service et neuf astronomes adjoints est adressé au début de l'année 1870 au ministre. À l'encontre du pouvoir discrétionnaire de Le Verrier, il mentionne «*les traitements devenus disponibles de M. Foucault, mort en février 1868, et de MM. Gruey et Lucas qui ont quitté l'Observatoire*». Les astronomes signataires démissionnent collectivement ; Le Verrier interpelle le ministre le 4 février 1870 et est destitué le 5 février. La brutalité des rapports que fait régner Le Verrier à l'Observatoire de Paris, le conflit entre les astronomes, parmi lesquels se trouve Lucas, et leur directeur, entraînent une réaction du directeur du laboratoire de chimie de l'École normale supérieure, Henri Sainte-Claire Deville, qui prend fermement parti pour Lucas auprès du ministre (lettre du 9 février 1867, A.N. F^{17} 22970).

[17] Voir [Tournès 1998].

[18] « *Depuis de longues années, un siècle, les Astronomes de l'Observatoire déterminent chaque jour à des heures fixes, la pression de l'atmosphère et la température de l'air. Ces déterminations sont indispensables pour la réduction des observations astronomiques quand il y en a* [...]. *Elles ont d'ailleurs, indépendamment de leur utilité propre pour la Science et l'Astronomie en particulier, le très grand avantage de garder à l'Observatoire la présence de l'un de MM. les observateurs ; et sans elles il arriverait que, dans les temps couverts, on pourrait être des semaines entières sans qu'aucun observateur parût à l'Observatoire, inconvénient grave à tous égards. J'étais*

La guerre franco-allemande interrompt l'activité scientifique de Lucas. Après avoir participé à la campagne de l'armée de la Loire, il sollicite une chaire de mathématiques dans un lycée parisien. Les raisons invoquées semblent surtout d'ordre scientifique : Lucas s'occupe alors de la publication d'une traduction d'un traité d'astronomie dont le premier volume seul est paru à ce moment-là[19] et «*souhaite être placé dans une situation qui lui permît de continuer ses travaux*», réclamations «*impossibles à admettre*» (note du ministère, août 1871). Malgré l'appui du directeur du laboratoire de chimie de l'École normale supérieure, Henri Sainte-Claire Deville[20], un « exil » en province lui est imposé. Sa nomination au lycée de Moulins comme professeur de mathématiques spéciales devient effective le 13 avril 1872. Il y demeure jusqu'en septembre 1876, et son mariage avec Marthe Boyron, fille d'un avocat parisien, a lieu pendant cette période provinciale (août 1873).

. . . mais une grande productivité scientifique

Lucas, professeur à Moulins, semble trouver dans cette ville la sérénité nécessaire à son travail scientifique. De 1873 à 1875, on peut noter ses interventions dans le *Bulletin de la Société d'émulation du département de l'Allier* et remarquer la qualité des publications qui voient le jour dans les années 1875 et 1876. On peut s'interroger sur les motivations historiques qui ont pu pousser Lucas à s'intéresser dès ces années-là aux travaux de Fermat et de Mersenne. C'est à Moulins en effet qu'il commence ses recherches arithmétiques et, vers la fin de son séjour provincial, paraissent

informé que depuis quelques temps ce travail se relâchait considérablement ; que des observations étaient déplacées d'une demi-heure et plus» (Lettre de Le Verrier au ministre de l'Instruction publique, 29 juillet 1868, A.N. F^{17} 22970).

[19] Il s'agit d'une traduction, en collaboration avec Charles André, du *Traité d'astronomie sphérique et d'astronomie pratique* de Brünnow (Dublin), paru chez Gauthiers-Villars en 1870. Le deuxième volume paraît en 1872. Lucas l'enrichit de notes, tables et développements nouveaux sur les méthodes allemandes.

[20] « *Cher ami, Vous savez que Lucas n'a pas fait bonne figure à l'observatoire sous l'administration Le Verrier. Il faut dire qu'il n'a guère été encouragé au travail par son directeur. Mais c'est un garçon bien fort et capable de bonnes choses, comme il en a produit plusieurs. Lisez sa lettre et jugez. Je serais bien heureux que vous puissiez le servir. Il est très ingénieux et son calcul des tissus est chose curieuse et utile. Ne rejetez pas trop facilement ce jeune homme. Vous savez que je vous dis toute la vérité : je vous l'ai prouvé récemment. Votre ami de cœur. H. Sainte-Claire Deville*» (Lettre de Sainte-Claire Deville au ministre de l'Instruction publique, 28 juillet 1871, A.N. F^{17} 22970). Le « *calcul des tissus*» fait référence à [Lucas 1867].

les premiers articles significatifs aussi bien dans les notes aux *Comptes rendus* de l'Académie des sciences, que dans les comptes rendus des congrès de l'AFAS. En 1876, commence la collaboration avec le *Bulletino di bibliografia e di storia* du prince Boncompagni et un premier échange épistolaire international a lieu en août avec Luigi Cremona[21]. L'intérêt de Lucas pour l'instrument arithmétique devient perceptible également en 1876, où il intervient pour la première fois au congrès de l'AFAS[22]. Au même congrès, Pafnuti Lvovich Tchebychef (selon une orthographe de l'époque) expose le principe d'une machine arithmétique additive à mouvement continu.

En cette année 1876, Lucas présente de Moulins deux thèses de mathématiques qui subissent quelques avatars si l'on en croit leur auteur[23] : faut-il y voir une certaine désinvolture du monde universitaire à l'égard d'un professeur de province ? Les deux thèses sont jugées dignes de l'approbation de la Faculté, pourtant aucune d'entre elles n'est soutenue[24]. Il est vraisemblable que la nomination tant souhaitée dans

[21] Voir *La corrispondenza di Luigi Cremona (1830-1903)*, paru dans les *Quaderni della Rivista di storia della scienza*, Università degli Studi di Roma « *La Sapienza* », vol. 1, Rome, 1992, p. 95–100.

[22] Ainsi, Lucas écrit le 30 juillet 1876 à la Direction de l'enseignement : « *Je dois exposer au Congrès de Clermont une* machine arithmétique *dont, je l'espère, on parlera dans quinze jours.* » Et le 18 septembre 1876 : « *J'ai inventé une* machine arithmétique *pour vérifier les nombres premiers de cent chiffres (le plus grand connu en a dix) qui a fait l'admiration de MM. Angelo Genocchi, de Turin, et Tchebycheff, de Saint-Pétersbourg ; je pense avoir* révolutionné *(c'est le vrai mot) l'arithmétique ; j'ai présenté cette année cinq mémoires à l'institut, deux thèses à la Sorbonne (qu'on a laissé traîner deux mois au Ministère)* » (A.N. F^{17} 22970).

Le congrès de Clermont est le congrès de l'AFAS de 1876, auquel participent, outre Tchebychef qui y fait cinq communications, Eugène Catalan [Jongmans 1996]. Lucas y fait quatre communications.

[23] Lucas écrit le 30 juillet 1876 à la Direction de l'enseignement : « *J'ai présenté une première thèse de mathématiques ; elle a été perdue ; j'en présente une seconde, et l'adresse directement au Ministre pour éviter l'ennui de la première, on m'accuse réception trois mois après l'avoir laissée dans les Bureaux* » (A.N. F^{17} 22970).

[24] La thèse de géométrie de Lucas porte « *Sur l'application du système de coordonnées tricirculaires et tétrasphériques à l'étude des propriétés des figures anallagmatiques* », celle d'arithmétique « *Sur l'application des séries récurrentes à la recherche des nombres premiers* ». Dans son appréciation sur la thèse de géométrie, Ossian Bonnet, le 3 décembre 1877, souligne que celle-ci « *quoique roulant sur un sujet élémentaire et relativement facile* [...] *contient un grand nombre de résultats nouveaux et intéressants, qui prouvent que l'auteur possède un véritable talent d'invention* ». Dans son rapport sur la thèse d'arithmétique, Charles Hermite, le 14 décembre 1877, loue « *des résultats*

un lycée parisien à l'automne 1876 rend cette soutenance inutile ; une thèse dans un domaine peu considéré en France ne peut conduire qu'à une carrière dans une faculté des sciences provinciale, situation alors beaucoup moins prisée qu'une chaire dans une classe préparatoire parisienne. Or le ministre de l'Instruction publique répond enfin favorablement aux requêtes de Lucas, qui n'a cessé depuis la fin de la guerre franco-allemande de solliciter une chaire dans un lycée parisien. La recommandation en août 1876 d'un député républicain récemment élu, Charles-Ange Laisant[25], peut avoir joué un rôle décisif. Le dossier scientifique de Lucas, qui s'enrichit chaque année de nouvelles publications, plaide aussi fortement en faveur de l'arithméticien. En tout état de cause, la compétition autour des postes parisiens demeure vive puisque, vers la fin de son séjour au lycée de Moulins, Lucas doit répondre à quelques accusations au moment où on lui promet «*la première chaire de mathématiques spéciales vacante à Paris*»[26]. Malgré son retour dans la capitale, et les avantages substantiels attachés à son nouveau poste, une certaine amertume devient perceptible dans sa correspondance :

«*Malheureusement, par système ou par négligence, les recherches arithmétiques qui sont considérées comme les plus difficiles ne sont pas en honneur en France, actuellement ; je les aurais abandonnées depuis longtemps si je n'avais eu le bonheur de rencontrer la protection et les encouragements de M. le Prince Boncompagni et de M. le Prince de Polignac*»[27].

Lucas est nommé professeur au lycée Charlemagne, où il enseigne de

nouveaux et extrêmement curieux sur la question difficile de la décomposition des nombres entiers en leurs facteurs premiers». Quoique adaptée à des cas très particuliers, la méthode est jugée élémentaire, mais en même temps originale et ingénieuse (A.N. AJ^{16} 5804).

[25] C.-A. Laisant (1841–1920) est admis en 1859 à l'École polytechnique ; capitaine du génie, il est élu député de Loire inférieure en 1876, de Paris en 1885 et en 1889 sous l'étiquette boulangiste. Il préside la Société mathématique de France en 1888 ; docteur ès-sciences, il est répétiteur (en 1895) puis examinateur à l'École polytechnique (en 1899). En 1899 il fonde avec H. Fehr la revue genevoise l'*Enseignement mathématique*. Il apparaît à l'AFAS en 1874 et préside celle-ci en 1904.

[26] Dans une lettre au Directeur de l'enseignement en date du 18 septembre 1876, Lucas se défend vivement d'être un professeur «*communard*». On y trouve entre autres cette profession de foi : «*Ne m'occupant aucunement de politique, n'ayant jamais assisté, même de loin, à ce que l'on appelle des réunions publiques, je préfère mon cabinet d'étude au forum, et n'ai point l'intention de devenir l'homme-berger ou l'homme-troupeau, les deux pôles de la politique*» (A.N. F^{17} 22970).

[27] Lucas au Directeur de l'enseignement, le 11 juillet 1877 (A.N. F^{17} 22970).

septembre 1876 à octobre 1878 en classe de mathématiques élémentaires, puis en mathématiques spéciales de 1878 à 1879. Une promotion rapide l'installe en mathématiques spéciales au lycée Saint-Louis en octobre 1879.

Il est difficile d'évaluer la qualité de l'enseignement de Lucas à la lumière des rapports d'inspection officiels[28]. On peut noter que son caractère de mathématicien original et de professeur très savant est reconnu : le cachet personnel qu'il imprime à son enseignement constitue un attrait pour les meilleurs élèves mais une difficulté pour «*les esprits médiocres*». Les cours de Lucas donnent l'habitude de «*suivre avec la plume*» les exercices faits au tableau, ce qui semble peu l'usage en d'autres classes. On lui sait gré de fournir gratuitement des leçons supplémentaires tous les dimanches matins aux élèves qui veulent venir chez lui. Par contre, la question du lien entre la recherche et l'enseignement rencontre beaucoup d'incompréhension de la part de l'administration et des parents d'élèves. Lucas a visiblement une difficulté à poursuivre ses travaux personnels tout en préparant ses élèves aux concours ; les succès dans sa section à l'entrée à l'École polytechnique seraient moindres que ceux de ses collègues. Le mot est lâché par l'inspection de 1878 au lycée Charlemagne : la manière de Lucas «*peut laisser craindre que chez lui les grandes recherches scientifiques ne fassent quelque tort à l'humble travail de la classe*». Au lycée Saint-Louis, après des débuts encourageants, une véritable cabale semble organisée contre lui. Le proviseur finit par céder aux pressions et insiste auprès du ministre en août 1890 sur la nécessité de déplacer M. Lucas «*qui a perdu la confiance des élèves et des familles*»[29]. Le retour de Lucas au lycée Charlemagne, en classe de mathématiques spéciales, prend effet en septembre 1890.

L'activité scientifique de Lucas ne ralentit pas pendant sa période parisienne (1876–1891). Notons qu'en 1877 il a déjà acquis assez d'autorité pour être nommé vice-président de la Commission des sciences mathématiques, à la réunion des délégués des sociétés savantes à la Sorbonne. L'examen de ses publications fait apparaître des années très productives

[28] A.N., F^{17} 22970 et AJ^{16} 1242.

[29] Le vice-recteur au ministre, le 13 août 1890. L'argument politique apparaît dans cette lettre : «*Il y aurait intérêt à remédier à cette situation, à un moment où nos lycées sont, dans une partie de l'opinion, l'objet d'une certaine défaveur. Il importe de ne négliger aucun moyen d'assurer notre clientèle pour le recrutement des Écoles*» (A.N., AJ^{16} 1242).

sur le plan scientifique : de 1875 à 1883 paraissent en effet 9 notes aux *Comptes rendus* de l'Académie des sciences, 11 articles pour le *Bulletin* de la Société mathématique de France ; les articles fondamentaux publiés dans des revues étrangères italiennes et américaine sont écrits principalement entre 1876 et 1879[30]. C'est dans cette période que l'on trouve le plus grand nombre de notes de Lucas dans les revues d'enseignement ou de vulgarisation. Le contenu des publications des dernières années, de 1884 à 1891, s'infléchit : la diffusion et la popularisation de la science deviennent les préoccupations majeures de l'arithméticien, comme en témoignent ses nombreuses récréations mathématiques et scientifiques[31]. Il semble vouloir rassembler ses visions théoriques dans son traité de *Théorie des nombres*, dont les volumes devaient réunir tant de travaux épars, mais à sa mort seul le premier d'entre eux est rédigé. Certaines œuvres, *Récréations mathématiques* ou *Arithmétique amusante*, seront publiées à titre posthume sous l'égide de la Société mathématique de France grâce aux efforts de H. Delannoy, C.-A. Laisant et E. Lemoine.

Dans le même temps, Lucas occupe des responsabilités importantes à l'AFAS[32] et continue de participer activement à ses congrès ; on lui doit 32 interventions dont une conférence générale au congrès de 1884 sur «*Le Calcul et les machines à calculer*». Il faut mentionner également l'action de Lucas en vue de la publication des œuvres de Fermat[33]. Ainsi, il obtient une mission en Italie, pour la recherche de manuscrits inédits, entre 1882 et 1883. Cette action aboutit après la mort de l'arithméticien

[30] Il s'agit de l'*American Journal* de Baltimore, des *Annali di matematica pura ed applicata* de Milan, des *Atti della reale Accademia dei Lincei* de Rome, des *Atti della reale Accademia della scienze di Torino*, et du *Bulletino* du prince Boncompagni.

[31] Dans la première période sont publiées 39 notes dans les *Nouvelles annales de mathématiques*, 21 dans la *Nouvelle correspondance mathématique* de Bruxelles, 7 dans le *Messenger of mathematics* de Cambridge, ainsi que 14 articles pour la *Revue scientifique de la France et de l'étranger*. Ultérieurement 10 notes paraissent dans la revue *Mathesis* de Bruxelles et 16 articles dans la revue de vulgarisation *La Nature*.

[32] Édouard Lucas est secrétaire des deux premières sections de l'AFAS, regroupant les mathématiques, l'astronomie, la géodésie et la mécanique, aux congrès du Havre (1877), de Paris (1878) et de Montpellier (1879). Il préside ces sections aux congrès de Reims (1880), de Nancy (1886) et de Marseille (1891). En octobre 1891, il est blessé accidentellement au cours du banquet qui fait suite au congrès de l'AFAS et meurt peu après d'un érysipèle. Veuf, il laisse deux enfants.

[33] L'AFAS émet un vœu en ce sens, assorti d'une demande de création en France d'une chaire de théorie des nombres en 1880, puis à nouveau en 1887 et 1888.

puisque les œuvres de Fermat sont publiées à partir de 1891 par Paul Tannery et Charles Henry sous les auspices du ministère de l'Instruction publique.

L'œuvre scientifique générale de Lucas peut s'apprécier à la lecture du premier volume de son traité de *Théorie des nombres*. Trois livres le composent : les nombres entiers, les nombres rationnels, la divisibilité arithmétique. Dans un échange épistolaire avec Ernesto Cesàro, l'auteur présente son travail encore sous presse en affirmant sa filiation :

«*Mon ouvrage est la glorification de cette trinité : Fibonacci, Fermat, Pascal ; ils avaient la vue longue ; on l'a si courte aujourd'hui*»[34].

Au travers de sa *Théorie des nombres*, l'auteur donne libre cours à des apports nombreux relevant de la «*géométrie de situation*» (réseaux, problème des quatre couleurs, polyèdres convexes), ou développant l'analyse combinatoire au profit du calcul des probabilités et le côté aléatoire de la théorie des jeux. Outre ces applications, on relève une étude très fine des fractions continues et une démonstration particulièrement élégante d'un théorème appelé réciproque du petit théorème de Fermat. Les propriétés des suites récurrentes, examinées dans le contexte de la divisibilité arithmétique, constituent un des chapitres essentiels de l'ouvrage : «*La théorie des suites récurentes est une mine inépuisable qui renferme toutes les propriétés des nombres*» [Lucas 1891a, p. xii]. Sur elles se fondent les méthodes de calcul rapide et les tests de primalité de l'auteur.

Malgré son activité diversifiée en faveur de l'avancement de la science des nombres, l'influence de Lucas reste peu importante en France. Son échec au Collège de France en témoigne. La demande de création d'une chaire d'arithmétique supérieure au Collège est faite à deux reprises par Laisant, l'ami de toujours, devant la Chambre des députés en 1887 et 1888. Le 9 mars 1888 Laisant intervient au cours de la discussion sur le budget, proposant d'élever de 10 000 francs la dotation du Collège de France «*pour la création d'une chaire de Théorie des nombres*» ; le nom de Lucas est avancé. La proposition est repoussée par les députés[35].

---

[34] Lettre de Lucas à Cesàro, du 4 octobre 1890, communiquée par le *Fondo Cesàro*, Dipartimento di Matematica «*R. Caccioppoli*», Università degli studi di Napoli «*Federico II*».

[35] Voir *Journal officiel aux débats de la Chambre*, discussion sur le budget de l'exercice 1888, 9 mars 1888 (2e séance).

SUR UNE CONTRIBUTION DE LUCAS : LES TESTS DE PRIMALITÉ

Les publications de Lucas relatives aux nombres premiers s'échelonnent des années 1875 à 1880, l'année 1876 étant l'année clé. Elles concernent les propriétés des suites récurrentes linéaires d'ordre deux[36] et de primalité[37]. Le mémoire italien [Lucas 1878b] est consacré à l'étude des nombres de Mersenne et, dans la note [Lucas 1880], Lucas compare ses résultats à ceux qu'obtient James Joseph Sylvester par l'utilisation de fonctions cyclotomiques [Sylvester 1880a].

Lucas dispose initialement de deux méthodes pour étudier la primalité des entiers, l'une due à Pierre de Fermat, l'autre à John Wilson, la première fournissant également une factorisation des nombres composés.

La caractérisation de la primalité de n par la méthode de Fermat repose sur la recherche de solutions entières de l'équation $x^2 - y^2 = n$. Pour que n soit premier, il faut et il suffit que l'équation de Fermat admette pour seules solutions $x = \frac{1}{2}(n+1)$ et $y = \frac{1}{2}(n-1)$:

« *Ainsi, pour qu'un nombre impair soit premier, il faut et il suffit qu'il soit, et d'une seule manière, égal à la différence des carrés de deux nombres entiers. De là cette méthode indiquée par Fermat pour reconnaître si un nombre impair donné n est premier ou composé. On ajoute au nombre n tous les carrés jusqu'à celui de* $\frac{1}{2}(n-1)$ *; si l'on ne trouve qu'un seul total, le dernier, égal à un carré, le nombre essayé est premier. Dans le cas contraire, le nombre est composé, et on le décompose immédiatement en un produit de deux facteurs* » [Lucas 1891a, p. 356].

Très coûteuse en opérations, cette méthode suppose l'utilisation de tables de carrés, donc demeure pratiquement inopérante pour les très grands nombres n.

Le théorème de Wilson est lui aussi remarquable en ce qu'il donne une condition nécessaire et suffisante de primalité. Publié en 1770 par Edward Waring qui l'attribue à John Wilson son élève, il n'est démontré par aucun

[36] Elles figurent dans les notes aux *Comptes rendus* [Lucas 1876a] et [Lucas 1876b], dans l'intervention au congrès de l'AFAS [Lucas 1876d] ainsi que dans les mémoires publiés en Italie [Lucas 1877c] et aux États-Unis [Lucas 1878a] ; elles sont reprises dans le traité [Lucas 1891a].

[37] Ces tests figurent dans les notes [Lucas 1876c], [Lucas 1877a], [Lucas 1877b], dans les interventions à l'AFAS [Lucas 1876d] et [Lucas 1877f], ainsi que dans [Lucas 1877c] et [Lucas 1878a].

de ces deux mathématiciens[38]. Sa formulation moderne est la suivante :

Un nombre n est premier si et seulement si le nombre $(n-1)!+1$ est divisible par n.

Lucas reproduit dans son traité la démonstration du théorème de Wilson selon la méthode de Lagrange (calcul des différences) et selon celle de Gauss (calcul par congruences). Sa conclusion est toutefois sans appel : «*Il est inapplicable en pratique*», le calcul du nombre factoriel $(n-1)!$, même modulo n, demeurant inaccessible pour les très grandes valeurs de n[39].

Le petit théorème de Fermat

La réflexion de Lucas s'oriente vers le théorème de Fermat, que l'on peut énoncer de la façon suivante[40] :

Si p est un nombre premier qui ne divise pas a, le nombre a^{p-1} est congru à 1 (mod. p).

Gauss contribue à l'amélioration de ce résultat :

«*Si p est un nombre premier qui ne divise pas a, et que a^t soit la plus petite puissance de a congrue à l'unité, l'exposant t sera $p-1$, ou une partie aliquote de $p-1$*» [Gauss 1807, *Disq.* n° 49].

Gauss établit ici que les entiers naturels x vérifiant l'équation $a^x \equiv 1$ (mod. p) sont les multiples du plus petit d'entre eux, noté t. Comme $p-1$ est l'un de ces entiers, il est un multiple de t (une «*partie aliquote*»

[38] Lagrange en 1771, Euler en 1783, Legendre en 1798 et enfin Gauss en donnent une démonstration. Voir [Waring 1770, p. 380], [Lagrange 1771], [Euler 1783, t.1, p. 329], [Legendre 1798, § 130 et 131, p. 167–168] et [Gauss 1830, *Disq.* n° 76–77].

[39] Voir [Lucas 1891a, p. 432 et p. 437–438]. Cette remarque est à rapprocher de celle de Legendre [1830, § 131] : «*Quoique cette règle soit très belle* in-abstracto*, elle ne peut guère être utile dans la pratique, attendu la grandeur énorme à laquelle s'élève bientôt le produit* $1 \cdot 2 \cdot 3 \cdots (n-1)$».

[40] Pour l'historique de ce théorème voir [Weil 1983]. Des démonstrations de ce résultat sont dues à Euler [1750, p. 67] et à Jean-Henri Lambert [1769, p. 109] ; Gauss soupçonne Leibniz d'avoir eu la même idée qu'Euler, mais sans l'avoir publiée. Gauss [1801, *Disq.* n° 49, 50, 51] établit la congruence $(a+b+\cdots+\ell)^p \equiv a^p+b^p+\cdots+\ell^p$ (mod. p) pour p premier, ce qui entraîne le théorème de Fermat si tous les nombres $a, b, \ldots, \ell$ sont supposés égaux à 1.

Lucas reproduit les démonstrations d'Euler et de Gauss avec un commentaire empreint de nationalisme : «*pour nous, il nous paraît impossible d'admettre que cette démonstration, si simple et si naturelle, trouvée par Leibniz, Euler et Lambert n'ait pu être imaginée par Fermat qui a non seulement énoncé le théorème, mais en a déduit de nombreux corollaires dont l'exactitude a été démontrée*» [Lucas 1891a, p. 420–423].

d'un nombre est un diviseur de ce nombre strictement inférieur à lui). Le raisonnement utilisé est celui qui, dans une terminologie moderne, entre en jeu pour établir que tout idéal de l'anneau des entiers est principal.

Euler élabore une généralisation du théorème de Fermat valable pour un entier n quelconque grâce au nombre $\varphi(n)$, appelé depuis l'indicateur d'Euler de n, qui désigne le nombre de nombres premiers avec n et inférieurs à n :

Si a et n sont premiers entre eux, on peut écrire $a^{\varphi(n)} \equiv 1$ (mod. n).

Si n est un nombre premier qui ne divise pas a, on retrouve le théorème de Fermat (dans ce cas en effet $\varphi(n) = n - 1$).

Pour sa part, Lucas fournit un exemple prouvant que le théorème de Fermat n'est pas caractéristique des nombres premiers ; il établit que $2^{37 \cdot 73 - 1} \equiv 1$ (mod. $37 \cdot 73$).

«*Cette congruence montre que le théorème de Fermat peut s'appliquer à des nombres composés et que, par conséquent, il n'a pas de réciproque*» [Lucas 1877f, p. 161] et [Lucas 1891a, p. 422–423].

Lucas effectue alors une synthèse entre les travaux de Fermat, Euler et Gauss [Lucas 1891a, p. 439–440]. Désignant par n un entier quelconque, il introduit la notion de «*gaussien*» de a selon le module n, lorsque a et n sont premiers entre eux : c'est le plus petit entier positif g tel que $a^g \equiv 1$ (mod. n) (à la différence du théorème de Gauss, l'entier n n'est pas supposé premier). Après avoir établi l'existence d'un élément minimal g parmi les solutions entières x de l'équation $a^x \equiv 1$ (mod. n), il montre que toutes les autres solutions x sont les multiples de g ; parmi elles se trouve l'indicateur d'Euler de n. Si la notion d'*idéal* est absente des écrits de Lucas, la modernité de son raisonnement nous frappe : c'est celui qui entre en jeu dans l'étude des anneaux principaux.

Lucas établit enfin le théorème qualifié de «*vraie réciproque*» du théorème de Fermat. La primeur de ce résultat théorique d'importance est offerte à l'AFAS : «*Nous avons énoncé pour la première fois ce théorème en 1876, au Congrès de l'Association Française pour l'Avancement des Sciences, à Clermont-Ferrand*» [Lucas 1891a, p. 441][41]. Il s'agit ici de reconnaître la primalité d'un entier p ; à cette fin, Lucas utilise un nombre

[41] Utiliser l'AFAS comme moyen de diffusion de recherches personnelles originales n'est pas une démarche habituelle au milieu scientifique français. Bien des communications de congrès de l'association sont en fait des rééditions de résultats publiés par ailleurs. Faut-il voir là une adhésion enthousiaste et militante de Lucas à la devise de l'AFAS :

intermédiaire a premier avec p et la suite $S_n = a^n - a$, pour laquelle il est affirmé :

«*Si on a S_n divisible par p pour $n = p$, et non auparavant, le nombre p est un nombre premier*» [Lucas 1876d, p. 63].

Autrement dit, si l'on peut construire une suite S_n du type précédent vérifiant (dans l'ensemble $\mathbb{Z}_p$ des entiers modulo p) les conditions $S_p \equiv 0$ et $S_n \not\equiv 0$ pour tout $n < p$, le nombre p est premier.

Une démonstration, qui repose sur un raisonnement par l'absurde, en est fournie dans l'*American Journal* [1878a, p. 231]. En supposant que p est un produit de facteurs premiers, par exemple $p = qr$, les propriétés de congruences permettent d'établir que $S_q \equiv S_r \equiv 0$ (mod. p) et p n'est pas le plus petit des indices n pour lequel S_n est divisible par p.

Ultérieurement, ce théorème prend la forme suivante[42] :

Les nombres a et p étant premiers entre eux, si $a^x - 1$ est divisible par p, pour x égal à $p - 1$, et n'est pas divisible par p pour x égal à une partie aliquote de $(p - 1)$, le nombre p est premier,
résultat que l'on peut exprimer ainsi :

Si l'on peut trouver un nombre a premier avec p, tel que la suite $s_n = a^n - 1$ vérifie (dans l'ensemble $\mathbb{Z}_p$ des entiers modulo p) les conditions $s_{p-1} \equiv 0$ et $s_d \not\equiv 0$ pour tout diviseur d de $p - 1$, le nombre p est premier.

Les conditions sont ici allégées, puisqu'elles portent sur les diviseurs de $p - 1$ et non sur tous les entiers inférieurs à p. La démonstration de ce résultat, beaucoup plus élégante que la précédente, fait appel au gaussien g de a selon le module p. En effet, si l'on constate que g est égal à $p - 1$, $\varphi(p)$ est aussi égal à $p-1$ en vertu de l'inégalité générale $g \leq \varphi(p) \leq p-1$, et par conséquent le nombre p est premier [Lucas 1891a, p. 441].

Ce théorème réciproque fournit un critère de primalité du nombre p, qui est d'un usage d'autant plus aisé que les diviseurs de $p-1$ sont rapidement accessibles, et que la recherche d'un a qui convienne, parmi les entiers

---

«*Par la science, pour la patrie*» et à ses objectifs : «*L'Association se propose de favoriser par tous les moyens en son pouvoir le progrès et la diffusion des sciences au double point de vue du perfectionnement de la théorie pure et du développement des applications pratiques*» ? [AFAS 1872, p. 2].

[42] Au Congrès de l'AFAS de 1877, ce théorème est déjà énoncé de cette manière (voir [Lucas 1877f, p. 162]). Des énoncés identiques figurent dans [Lucas 1878a, p. 302] et [Lucas 1891a, p. 441].

premiers avec p, est facile. Lucas peut ainsi vérifier que le nombre de Fermat $F_4 = 2^{2^4} + 1 = 65537$ est premier en 17 étapes seulement[43]. Il faut remarquer que, p étant premier, les conditions données par Lucas $a^{p-1} \equiv 1$ et $a^d \not\equiv 1 \pmod{p}$ pour tout diviseur d de $p-1$ signifient que a est racine primitive $(p-1)$-ième de l'unité dans le corps $\mathbb{Z}_p$ des entiers modulo p. La difficulté consiste à déterminer un nombre a convenable pour de très grands nombres p dont on cherche à établir la primalité (de nos jours, il n'existe aucune méthode systématique autre que la recherche exhaustive pour trouver les racines primitives de l'unité dans $\mathbb{Z}_p$)[44].

Les possibilités offertes par ce test sont peu exploitées par son auteur. Outre la difficulté à déterminer un nombre a qui convienne, la rapidité de la méthode est loin d'être assurée pour les très grands entiers p. Le calcul des nombres S_n ou s_n, même modulo p, devient en effet rapidement inextricable, sauf à disposer de procédures «*mécaniques*» qui n'apparaissent pas ici pour un nombre p de nature quelconque, ni pour des nombres particuliers comme ceux de Fermat (F_4 semble être le plus grand examiné par l'auteur sans ces procédures). Lucas s'intéresse aux nombres de Mersenne $M_n = 2^n - 1$ pour des raisons historiques[45], mais aussi parce que l'étude de leur primalité lui révèle une procédure de calcul automatique plus générale. Cette procédure utilise la suite de Fibonacci.

---

[43] Les nombres de Fermat sont les nombres $F_n = 2^{2^n} + 1$. Pour étudier F_4, Lucas utilise $a = 3$; les diviseurs de $F_4 - 1$ étant $1, 2, 2^2, \ldots, 2^{16}$, une récurrence simple peut être établie entre les restes dans la division par F_4 des nombres 3^{2^k} (si l'on a $3^{2^k} \equiv r_k$, $r_{k+1} \equiv r_k^2$, modulo 65537). Voir [Lucas 1891a, p. 441].

[44] Tout nombre a premier avec un nombre n n'est évidemment pas une racine primitive $(n-1)$-ième de l'unité dans $\mathbb{Z}_n$. Pour s'en convaincre, il suffit d'examiner le cas de $n = 7$: les racines primitives 6-ième de l'unité dans le corps $\mathbb{Z}_7$ sont 3 et 5 (il y en a exactement $\varphi(6) = 2$). Par contre, dans ce corps, 2 n'est pas une racine primitive 6-ième puisque $2^3 \equiv 1 \pmod{7}$, bien que 2 soit premier avec 7. Le test de Lucas est en défaut si l'on choisit $a = 2$ pour tenter d'établir la primalité de 7; celle-ci est par contre établie par le choix de $a = 3$ ou 5. A contrario, s'il existe un nombre a premier avec n vérifiant $a^{n-1} \not\equiv 1 \pmod{n}$, le nombre n est composé. Malheureusement, il existe des nombres n composés pour lesquels $a^{n-1} \equiv 1 \pmod{n}$ pour tout a premier avec n : ce sont les nombres de Carmichael (le nombre 561 en est un). La question du polynôme cyclotomique est liée aux précédentes : dans un corps donné, le polynôme cyclotomique d'ordre k est celui dont les zéros sont les racines primitives k-ièmes de l'unité. Pour toutes ces questions, voir [Warusfel 1971, p. 184] et [Demazure 1997].

[45] L'un des objectifs de Lucas est, en particulier, de savoir «*si les assertions du Père Mersenne et du Baron Plana* [...] *sur les nombres* $2^{53} - 1$, $2^{67} - 1$, $2^{127} - 1$, $2^{257} - 1$ *qu'ils considéraient comme premiers, sont exactes*» [Lucas 1877c, p. 162].

La loi d'apparition des nombres premiers dans la suite de Fibonacci

La suite de Léonard de Pise (connu sous le nom de Fibonacci) est régie par la relation de récurrence $u_{n+2} = u_{n+1} + u_n$. L'expression de son terme général dépend du choix des deux premiers termes u_0 et u_1, que Fibonacci prend égaux respectivement à 0 et 1 ; on obtient ainsi la suite de nombres 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55...

Lucas consacre à Léonard de Pise un copieux mémoire publié en Italie [Lucas 1877c]. L'attention aux propriétés arithmétiques de la suite de Fibonacci, qui remonte à Fermat, Frenicle (et probablement à des mathématiciens antérieurs), a pu être suscitée par une note de Gabriel Lamé [1844], où apparaît son utilité pour la détermination d'une limite supérieure du nombre des opérations à faire dans la recherche du plus grand commun diviseur de deux nombres entiers, ainsi que par les travaux arithmétiques d'Angelo Genocchi [1868–1869].

L'apport original de Lucas consiste à souligner une propriété arithmétique remarquable de cette suite : tout nombre premier p y figure en tant que facteur d'un terme de rang déterminé. C'est la *loi d'apparition des nombres premiers* au sein de la suite de Fibonacci[46].

On peut noter que la recherche de nombres premiers au sein de suites arithmétiques paraît bien antérieure à ces travaux. Ainsi Euler [1769, p. 113–126] et [1774, p. 263–266] s'intéresse à la présence des nombres premiers au sein de la progression arithmétique $4n + 1$. Legendre croit prouver en 1785 qu'«*il y a une infinité de nombres premiers compris dans toute progression arithmétique dont le premier terme et la raison sont premiers entre eux* [...] *Cette proposition est assez difficile à démontrer, cependant on peut s'assurer qu'elle est vraie. Je me contente d'indiquer ce moyen de démonstration qu'il serait trop long de détailler...* » [Legendre 1785, p. 552]. Hélas la démonstration de Legendre est fausse et cette proposition n'est réellement prouvée qu'en 1837 par Peter Gustav Lejeune-Dirichlet au moyen de méthodes analytiques[47].

Les travaux de Tchebychef sont eux aussi bien connus de Lucas.

[46] On peut signaler qu'un nombre premier « *apparaît* » au sein de plusieurs termes u_n ; la « *loi* » de Lucas permet de le repérer dans un terme au moins (qui n'est pas toujours celui de rang minimal). Ainsi 11 divise le terme $u_{10} = 55$, tandis que 17 divise $u_{18} = 2584$ (mais aussi $u_9 = 34$) et 5 divise $u_5 = 5$.

[47] Voir [Lejeune-Dirichlet 1837, p. 108–111]. On peut signaler qu'à ce propos Lejeune-Dirichlet se réfère à un texte d'Euler [1748].

Dans un *Mémoire sur les nombres premiers* présenté en 1850 à Saint-Pétersbourg, Tchebychef établit à son tour, en utilisant des méthodes analytiques, que, pour $a > 3$, il y a au moins un nombre premier plus grand que a et plus petit que $2a-2$, *postulatum* (le terme est de Tchebychef [1852]) dû à Joseph Bertrand [1845].

La recherche de nombres premiers au sein de suites est donc dans l'air du temps depuis des décennies lorsque, au congrès de l'AFAS de 1877, Lucas fait la remarque suivante :

«*En résumé, toutes ces recherches sont basées sur la considération des progressions arithmétiques. On doit à l'illustre Fermat des recherches profondes sur la doctrine des nombres premiers et basées sur la considération des problèmes des progressions géométriques. Dans cet ordre d'idées, différent de celui qui précède, la vérification des nombres premiers très-grands de la forme* $a^n - b^n$*, et la décomposition des nombres de cette forme en facteurs premiers, se trouve considérablement simplifiée*» [Lucas 1877f, p. 161].

Le sens de cette remarque apparaît dès que l'on exprime le terme général de la suite de Fibonacci en fonction de l'indice n. Cette expression met en jeu l'équation caractéristique $r^2 - r - 1 = 0$ liée à la relation de récurrence $u_{n+2} = u_{n+1} + u_n$. Le discriminant de cette équation est 5, ce qui confère au nombre 5 un rôle particulier dans toute l'étude qui suit. Les racines de cette équation caractéristique étant $a = \frac{1}{2}(1 + \sqrt{5})$ et $b = \frac{1}{2}(1 - \sqrt{5})$, le terme de rang n de la suite de Fibonacci s'écrit $u_n = (a^n - b^n)/(a - b)$, sachant que $u_0 = 0$ et $u_1 = 1$.

La parenté avec les suites utilisées dans le théorème réciproque de Fermat ($S_n = a^n - a$ ou $s_n = a^n - 1$) est évidente, toutes ces suites étant liées aux suites géométriques. Leur croissance rapide permet une utilisation, pour l'étude des très grands nombres premiers, plus satisfaisante que celle des suites arithmétiques présentes dans les résultats de Legendre ou Lejeune-Dirichlet.

Les propriétés arithmétiques de la suite de Fibonacci sont énoncées dans de nombreuses publications, notamment au congrès de l'AFAS de 1876 [Lucas 1876d, p. 64–65] et dans l'*American Journal* [Lucas 1878a, p. 296–297]. La plus fondamentale demeure la loi d'apparition des nombres premiers, qui est constituée des résultats suivants :

2 divise u_3, ainsi que tous les termes dont l'indice est un multiple de 3 ;

5 divise u_5, ainsi que tous les termes dont l'indice est un multiple de 5.

Si p est un nombre premier non égal à 2 ou 5, on a $u_{p-1} \equiv 0$ ou $u_{p+1} \equiv 0$ (mod. p) selon que 5 est ou non résidu quadratique de p[48].

Si p est un nombre premier non égal à 5, $u_p \equiv \pm 1$ (mod. p).

La démonstration de ces propriétés apparaît dans l'*American Journal*. Elle repose sur l'utilisation de la formule du binôme de Newton dans le corps quadratique $\mathbb{Q}[\sqrt{5}]$ pour le calcul des quantités $(1+\sqrt{5})^n$ et $(1-\sqrt{5})^n$. Le terme de rang n de la suite de Fibonacci s'en déduit : $2^{n-1}u_n = C_n^1 + 5C_n^3 + 5^2C_n^5 + \cdots + 5^{(k-1)/2}C_n^k + \cdots$, la somme étant étendue à tous les entiers impairs $k \leq n$. Le calcul se poursuit dans le corps $\mathbb{Z}_p$ (p est un nombre premier impair) où les coefficients binomiaux ont des formes particulièrement simples pour $n = p-1, p$ et $p+1$[49]. Les valeurs des termes de rang $p-1$, p, $p+1$ de la suite de Fibonacci en résultent puisque : $2^p u_{p-1} \equiv 1 - 5^{(p-1)/2}$, $2^{p-1}u_p \equiv 5^{(p-1)/2}$ et $2^p u_{p+1} \equiv 1 + 5^{(p-1)/2}$. Le théorème de Fermat est nécessaire pour écrire $2^{p-1} \equiv 1$, et les résultats concernant les résidus quadratiques ($5^{(p-1)/2} \equiv \pm 1$ selon que 5 est ou non résidu quadratique de p si p n'est pas égal à 5) permettent de conclure.

La loi d'apparition des nombres premiers au sein de la suite de Fibonacci trouve une expression quelque peu différente dans certaines publications, ainsi[50] :

« *Dans la série de Fibonacci, tout nombre premier p impair, de la forme* $10q \pm 1$*, divise le terme de rang* $p-1$*, et tout nombre premier impair de la forme* $10q \pm 3$*, divise le terme de rang* $p+1$*. D'ailleurs les nombres* 2 *et* 5 *divisent respectivement tous les termes dont le rang est un multiple de* 3 *ou de* 5 » [Lucas 1878a, p. 297] .

Bien d'autres suites ont la propriété de « *faire apparaître tous les nombres premiers* ». Ainsi la suite de Pell utilisée parfois par Lucas est définie par la relation de récurrence $u_{n+2} = 2u_{n+1} + u_n$ ($u_0 = 0$, $u_1 = 1$).

---

[48] On dit que 5 est ou non résidu quadratique de p premier selon que l'équation $x^2 = 5$ admet ou non une solution dans le corps $\mathbb{Z}_p$ des entiers modulo p, c'est-à-dire selon que le polynome $x^2 - 5$ se factorise ou non dans $\mathbb{Z}_p[X]$. Si 5 est résidu quadratique de p, on a $5^{(p-1)/2} \equiv 1$ (mod. p) ; sinon on a $5^{(p-1)/2} \equiv -1$.

[49] Dans le corps des entiers modulo p, Lucas utilise $C_{p-1}^k \equiv (-1)^k$ pour $k = 0, \ldots, p-1$; $C_p^k \equiv 0$ pour $k = 1, \ldots, p-1$; $C_{p+1}^p = C_{p+1}^1 \equiv 1$ et $C_{p+1}^k \equiv 0$ pour $k = 2, \ldots, p-1$.

[50] On trouve des expressions semblables dans [Lucas 1876a, p. 166–167] et [Lucas 1877c, p. 149]. D'autres propriétés « *amusantes* » de la suite de Fibonacci sont signalées : ainsi tous les termes de rang impair sont la somme de deux carrés, et tous les termes, dont le rang pair est au moins 6, sont composés.

Les racines de l'équation caractéristique qui lui est associée ($r^2-2r-1=0$) s'expriment dans le corps $\mathbb{Q}[\sqrt{2}\,]$ et les propriétés de la suite de Pell s'énoncent de la même façon que celles de Fibonacci, le nombre 5 devant ici être remplacé par 2.

À toutes ces suites correspondent des équations caractéristiques dont les racines a et b s'expriment en général dans une extension quadratique de $\mathbb{Q}$ faisant intervenir leur discriminant Δ. Le succès de la méthode réside dans l'utilisation de cette extension : un nombre premier p apparaît dans le terme de rang $p-1$ ou $p+1$, si p n'est pas égal à Δ.

Dans le cas où Δ est résidu quadratique de p, c'est-à-dire où $\sqrt{\Delta}$ est un entier de $\mathbb{Z}_p$, cette loi d'apparition n'est autre que le théorème de Fermat appliqué au terme de rang $p-1$ de la suite considérée : en effet les racines a et b de l'équation caractéristique sont alors des entiers de $\mathbb{Z}_p$, qui vérifient le théorème de Fermat $a^{p-1} \equiv b^{p-1} \equiv 1$ ce qui entraîne $u_{p-1} \equiv 0 \pmod{p}$ en vertu de l'expression du terme général de la suite u_n. Dans le cas contraire, $\sqrt{\Delta}$ n'est pas un entier de $\mathbb{Z}_p$; les racines a et b de l'équation caractéristique sont dans $\mathbb{Q}[\sqrt{\Delta}\,]$ et l'apport de Lucas consiste à remarquer la présence de p au sein du terme de rang $p+1$ de la suite considérée. Ce résultat lui a été inspiré par un lemme de Joseph Lagrange[51], qui permet en effet d'écrire $u_{p+1} \equiv 0 \pmod{p}$, lorsque le discriminant Δ de l'équation caractéristique n'est pas un carré parfait dans $\mathbb{Z}_p$.

En effectuant une synthèse entre les résultats de Fermat et Lagrange, la méthode de Lucas élargit le champ d'application du théorème de Fermat. L'utilisation de suites exprimées dans une extension quadratique de $\mathbb{Q}$, au lieu de $\mathbb{Z}$, ouvre deux possibilités au lieu d'une seule pour l' «*apparition*» d'un nombre premier p. Les tests de primalité qui en découlent permettent ainsi d'examiner aussi bien des nombres de Mersenne (2^n-1) que de Fermat $(2^{2^n}+1)$.

Les tests de primalité associés à la suite de Fibonacci

On trouve dans [Lucas 1878a, p. 302] le critère de primalité suivant : «*Si dans l'une des séries récurrentes u_n, le terme u_{p-1} est divisible par p,*

[51] À propos de la loi d'apparition des nombres premiers, Lucas précise en effet [1876b, p. 1304] que, si δ^2 désigne le discriminant de l'équation caractéristique associée à la suite récurrente, « *cette loi a été donnée par Fermat, lorsque δ est rationnel, et par Lagrange, lorsque δ est irrationnel*». Nous renvoyons le lecteur au lemme VII de Lagrange [1775, p. 782].

sans qu'aucun des termes de la série dont le rang est un diviseur de $p-1$ *le soit, le nombre p est premier ; de même, si* u_{p+1} *est divisible par p, sans qu'aucun des termes de la série dont le rang est un diviseur de* $p+1$ *le soit, le nombre p est premier*»[52].

La démonstration de ce résultat, qui constitue une condition suffisante de primalité, repose sur les propriétés suivantes de la suite de Fibonacci :

1) La propriété de Lucas : les diviseurs de u_{m+n} et u_n sont identiques à ceux de u_m et u_n.

2) La propriété de Genocchi : si d désigne le pgcd de m et n, u_d est le pgcd de u_m et u_n ; en particulier, si m et n sont premiers entre eux, il en est de même de u_m et u_n.

3) Le terme u_{pq} est divisible par u_p et par u_q, donc par leur produit si p et q sont premiers entre eux.

Lucas semble avoir eu quelques difficultés à établir la démonstration de la propriété de Genocchi : celle qui figure dans les *Recherches sur plusieurs ouvrages de Léonard de Pise* [1877c, p. 140] nous paraît pour le moins heuristique. Elle s'est consolidée dans l'*American Journal* [1878a, p. 200–206] grâce à la théorie algébrique des fonctions numériques simplement périodiques.

À la suite $u_n = (a^n - b^n)/(a-b)$ (de premiers termes 0 et 1) , Lucas associe la suite $v_n = a^n + b^n$ (de premiers termes 2 et 1) dans lesquelles a et b désignent les racines de l'équation $r^2 - r - 1 = 0$. Ces suites obéissent toutes deux à la loi de récurrence de Fibonacci : un terme de rang n est la somme des deux termes de rang précédent[53]. La relation $2u_{m+n} = u_m v_n + u_n v_m$ peut être établie de manière élémentaire, et la propriété de Lucas en résulte, malgré une erreur de son auteur (Robert Carmichael est intervenu pour rectifier la démonstration[54]). Pour établir

[52] Ce critère est énoncé de manière très voisine dans [Lucas 1877c, p. 153]. Dans [Lucas 1876b, p. 1304] [Lucas 1876d, p. 66] et [Lucas 1877a, p. 440], on trouve le résultat suivant : «*si* $u_{p\pm1}$ *est divisible par p sans qu'aucun des termes dont le rang est un diviseur de* $p \pm 1$ *le soit, le nombre p est premier*».

[53] Ces suites u_n et v_n, auxquelles Lucas donne le nom de «*simplement périodiques*» en raison de propriétés algébriques qui les rapprochent de $\cos n$ et de $\sin n$, apparaissent chez Joseph Lagrange dans la résolution d'un problème de Fermat : «*étant donné un nombre entier quelconque non carré, trouver un nombre entier carré tel que le produit de ces deux nombres augmenté d'une unité soit un nombre carré*» [Lagrange 1766–1769, p. 693–695].

[54] Lucas utilise la propriété suivante : u_n et v_n sont premiers entre eux [Lucas 1878a,

la propriété de Genocchi, le résultat de Lucas est nécessaire ainsi qu'une récurrence «*descendante*» usuelle dans la recherche du pgcd. La troisième propriété est une simple conséquence de celle de Genocchi.

La démonstration du critère de primalité énoncé ci-dessus utilise les propriétés précédentes suivies d'un simple raisonnement par l'absurde ; elle figure dans la communication faite au Congrès de l'AFAS de 1876 [Lucas1876d, p. 66] et dans l'*American Journal* [Lucas 1878a, p. 302].

Il faut remarquer que le test qui résulte de ce critère n'est vraiment efficace que si les diviseurs de $p+1$ ou de $p-1$ sont accessibles, ce qui est le cas en particulier des nombres de Mersenne et de Fermat.

Pour mettre en œuvre ce critère de manière rapide, Lucas utilise deux propriétés élémentaires des suites précédentes : 1) $u_{2n} = u_n \cdot v_n$ et 2) $v_{2n} = v_n^2 - 2(-1)^n$ (la deuxième relation utilise le fait que $ab = -1$). On y voit apparaître le doublement des indices de chacune des suites, ce qui rend particulièrement aisé le calcul de proche en proche de leurs termes de rang pair. L'exemple en est fourni par l'étude des nombres de Mersenne et de Fermat.

Les nombres de Mersenne

Le nombre de Mersenne $M_n = 2^n - 1$ ne peut être premier si n n'est pas premier, mais la primalité de n ne suffit pas à entraîner celle de M_n. Pour tester la primalité de $p = M_n$, on peut tenter d'appliquer le critère de Lucas au rang $p+1$, les diviseurs de $p+1$ étant en évidence. Les conditions de primalité de p s'expriment alors dans l'anneau $\mathbb{Z}_p$ des entiers modulo p par les conditions portant sur la première suite : $u_{2^n} \equiv 0$ et $u_{2^k} \not\equiv 0$ pour tout entier $k \leq n-1$. En utilisant les propriétés 1) et 2) précédentes, ces conditions se transmettent à la deuxième suite : $v_{2^{n-1}} \equiv 0$ et $v_{2^k} \not\equiv 0$ pour tout entier $k \leq n-2$. En considérant enfin la suite $w_k = v_{2^k}$, de premier terme $w_1 = v_2 = 3$, dont les termes s'obtiennent de proche en proche (grâce à 2)) par $w_k = w_{k-1}^2 - 2$, on arrive à la formulation :

Pour tester la primalité de $p = 2^n - 1$, on forme la suite de nombres $w_1 = 3$, $w_2 = 7$, $w_3 = 47$, $w_4 = 2207, \ldots, w_k = w_{k-1}^2 - 2, \ldots$ Si le premier des termes divisibles par p est de rang égal à $n-1$, le nombre p est premier[55].

p. 200], malheureusement fausse pour tous les termes dont le rang est un mutiple de 3 ($u_3 = 2$ et $v_3 = 4$ par exemple). Le raisonnement rectifié est dans [Carmichael 1913].

[55] Ce critère est formulé dans [Lucas 1877f, p. 162] et [Lucas 1878a, p. 310].

Un commentaire présente cette méthode comme étant la seule «*directe et pratique connue actuellement*» pour la vérification des grands nombres premiers [Lucas 1878a, p. 303–304]. Les différentes opérations sont indépendantes de la construction préalable d'une table de nombres premiers, souvent entâchée d'erreurs, et par conséquent la méthode se trouve «*affranchie de l'incertitude de ces calculs numériques*»[56]. La puissance et la rapidité du test reposent sur la possibilité de doublement de l'indice : il suffit ainsi de vérifier les propriétés des nombres w_k aux rangs $k \leq n-1$, pour étudier le nombre $p = 2^n - 1$.

Lucas donne quelques exemples[57] d'application de son test : étude de la primalité de $2^{4q+3} - 1$, de $2^{4q+1} - 1$, de $2^{19} - 1$, de $2^{31} - 1$. À propos du nombre $2^{127} - 1$, il précise : «*J'ai ainsi vérifié, mais une seule fois, je l'avoue, que le nombre* $A = 2^{127} - 1$ *est premier*» [Lucas 1877c, p. 152]. Et plus loin : «*J'ai employé pour ce dernier nombre le système de la numération binaire, en opérant sur un échiquier de* 127 *cases de côté* [...] *Ce procédé a été employé, en partie du moins, par les mathématiciens arabes*» [Lucas 1877c, p. 158].

Les nombres de Fermat

Ce sont les nombres que nous noterons avec Lucas $a_n = 2^{2^n} + 1$. Fermat avait conjecturé leur primalité pour tous les indices n, ce qui est faux : Euler montre en 1732 le caractère composé de a_5 en trouvant le facteur 641.

---

[56] La comparaison est faite avec la méthode d'Euler : « *Cette méthode de vérification des grands nombres premiers, qui repose sur le principe que nous venons de démontrer, est la seule méthode directe et pratique, connue actuellement, pour résoudre le problème en question ; elle est opposée, pour ainsi dire, à la méthode de vérification d'Euler* [...] *Dans celle-ci, on divise le nombre soupçonné premier, par des nombres inférieurs à sa racine carrée* [...] *; le dividende est constant, et le diviseur variable. C'est l'insuccès de ces divisions dont le nombre est considérable* [...] *qui conduit à affirmer que le nombre essayé est premier. Dans notre méthode, au contraire, on divise, par le nombre soupçonné premier, des nombres d'un calcul facile* [...] *; ici le dividende est variable et le diviseur constant* [...] *; en outre, le nombre des opérations est peu considérable ; c'est le succès de l'opération qui conduit à affirmer que le nombre essayé est premier*» [Lucas 1878a, p. 303–304]. Un commentaire analogue figure dans [Lucas 1877c, p. 157].

[57] Pour $2^{4q+3} - 1$, voir par exemple [Lucas 1878a, p. 305] ; pour $2^{4q+1} - 1$, voir [Lucas 1878a, p. 316] ; pour $2^{19} - 1$, voir [Lucas 1877a, p. 441–442] ; pour $2^{31} - 1$, voir [Lucas 1876d, p. 66–67], [Lucas 1877c, p. 158] et [Lucas 1878a, p. 306–308].

«*Pour savoir si le nombre* $a_6 = 2^{2^6} + 1$ *est premier ou composé, l'application de toutes les méthodes connues jusqu'à présent* [...] *nécessiterait trois mille ans de travail assidu. Par le procédé suivant, il suffit de former successivement les carrés de soixante nombres ayant vingt chiffres au plus ; ce calcul peut être effectué en trente heures* [...] *Je fais effectuer en ce moment les calculs concernant* a_6 *et* a_7 » [Lucas 1877b, p. 137–138][58].

Le procédé de Lucas est appliqué ici au rang $p-1$, en posant $p = 2^{2^n}+1$. Il consiste à utiliser des suites de Pell, $u_{n+2} = 2u_{n+1}+u_n$, ce qui ne change pas fondamentalement la méthode précédente. Elles ont pour équation caractéristique $r^2 - 2r - 1 = 0$. Si a et b désignent les racines de cette équation, Lucas considère ici $u_n = (a^n - b^n)/(a - b)$, $v_n = \frac{1}{2}(a^n + b^n)$, $w_n = v_{2^n}$. Les suites u_n, v_n et w_n ont des propriétés analogues à ce qui a été vu plus haut, les calculs s'effectuant dans le corps quadratique $\mathbb{Q}[\sqrt{2}\,]$; en particulier, on a les relations $u_{2n} = 2u_n \cdot v_n$, $v_{2n} = 2v_n^2 - (-1)^n$ et $w_n = 2w_{n-1}^2 - 1$ (le premier terme étant ici $w_1 = 3$), ce qui permet l'énoncé suivant :

«*Soit le nombre* $a_n = 2^{2^n} + 1$ *; on forme la série des* $2^n - 1$ *nombres* $3, 17, 577, 665857, 886731088897, \ldots$, *tels que chacun d'eux est égal au double du carré du précédent diminué de l'unité ; le nombre* a_n *est premier, lorsque le premier terme divisible par* a_n *occupe le rang* $2^n - 1$ *; il est composé, si aucun des termes de la série n'est divisible par* a_n » [Lucas 1877b, p. 138][59].

Dans le rapport sur la thèse d'arithmétique de Lucas, Charles Hermite constate que les procédures proposées sont d'une utilisation aisée pour certaines catégories de nombres N seulement (ceux pour lesquels les diviseurs de $N \pm 1$ sont d'un accès facile). Le succès de leur application aux nombres de Mersenne et Fermat en particulier en découle, mais leur généralisation est malaisée.

Une autre critique est faite dès la publication des résultats d'Édouard Lucas par ses contemporains : ses méthodes constituent des conditions

[58] Les artisans de ces calculs pourraient bien être les élèves du lycée de Moulins ! Le nom de l'un d'entre eux est cité dans [Lucas 1877c, p. 158–159].

[59] Signalons qu'une erreur de calcul fait écrire à Lucas 2^{n-1} au lieu de $2^n - 1$; la méthode est donc moins rapide qu'il ne l'affirme. L'étude des premiers nombres de Fermat par la méthode de Lucas demande de nos jours quelques heures de travail avec le secours d'une calculette élémentaire non programmable.

suffisantes de primalité des nombres auxquels on les applique. Les tests qui en résultent peuvent faire apparaître des cas d'incertitude (en langage moderne, on peut parler à ce propos d'algorithmes semi-décidables ; ainsi le procédé préconisé conduit au cas d'incertitude pour l'étude de a_3 et a_4). Leur transformation en conditions nécessaires et suffisantes est posée par Théophile Pépin[60] qui énonce le *critérium* suivant :

«*La condition nécessaire et suffisante pour que le nombre* $a_n = 2^{2^n} + 1$ *soit premier, quand n est* > 1*, est que le nombre* $5^{(a_n-1)/2}+1$ *soit divisible par* a_n» [Pépin 1877, p. 329].

On forme donc la suite des nombres $5^2, 5^4, 5^8, \ldots, 5^{2^{2^n-1}}$ composée de $2^n - 1$ termes dont chacun est le carré du précédent mais «*on aura soin de réduire chaque terme à son résidu minimum suivant le module* a_n» (le calcul est effectué dans $\mathbb{Z}_p$ où $p = a_n$). Le nombre a_n est premier ou composé selon que le reste du dernier terme se réduit ou non au nombre $a_n - 1$. Le choix du nombre 5 est justifié par le fait que 5 n'est pas résidu quadratique de a_n ; il peut tout aussi bien être remplaçé[61] par 10.

En ce qui concerne les méthodes d'investigation de Lucas, la préface du traité de *Théorie des nombres* nous livre quelques réflexions sur le rôle de l'observation dans la science arithmétique[62].

---

[60] «*Les Comptes Rendus du* 16 *juillet dernier renferment une méthode ingénieuse pour reconnaître si le nombre* $a_n = 2^{2^n} + 1$ *est premier ou composé. Il est un cas cependant où l'emploi de cette méthode laisserait la question indécise* [...] *Néanmoins cette question peut être résolue sans incertitude par une méthode analogue à celle de M. Lucas*» [Pépin 1877, p. 329].

[61] Voir [Pépin 1877, p. 329–330]. Outre le théorème de Fermat et le calcul par congruences, Pépin utilise la loi de réciprocité de Legendre-Jacobi. Il poursuit ses recherches en fournissant en 1878 une condition nécessaire et suffisante de primalité des nombres de Mersenne $2^n - 1$. Sa méthode s'inspire de celle de Lucas en ce qu'elle repose sur la construction d'une suite récurrente du type $w_{k+1} = w_k^2 - 2$, mais dont le premier terme est fonction de l'entier n. Dans le *critérium* de Pépin, la détermination de ce premier terme n'est pas parfaitement explicitée [Pépin 1878].

Les suites de Pépin demeurent peu adaptées au calcul rapide et difficiles à construire. Lucas peut écrire en 1877 au Congrès de l'AFAS (p.165) que «*si la voie indiquée par le P. Pépin conduit à une forme plus claire et plus précise, donnant, comme le théorème de Wilson, la condition nécessaire et suffisante pour que le nombre* a_n *soit premier, il paraît cependant préférable de s'en tenir, dans l'application, à la forme ambiguë et indécise que nous avons laissée*» [Lucas 1877f, p. 165].

[62] Voir [Echeverria 1992] et [Echeverria 1996] qui traitent de l'aspect expérimental de la théorie des nombres au XIX$^{\text{e}}$ siècle. Ces références sont dues à l'obligeance de C. Goldstein.

«*Comme toutes les sciences, l'Arithmétique résulte de l'observation ; elle progresse par l'étude des phénomènes numériques donnés par les calculs antérieurs, ou fabriqués, pour ainsi dire, par l'expérimentation.* [...] *C'est par l'observation du dernier chiffre dans les puissances successives des nombres entiers que Fermat* [...] *créa l'Arithmétique supérieure, en donnant l'énoncé d'un théorème fondamental ; c'est par la méthode expérimentale, en recherchant la démonstration de cette proposition, que la théorie des racines primitives fut imaginée par Euler ; c'est par l'emploi immédiat de ces racines primitives que Gauss obtint son célèbre théorème sur la division de la circonférence en parties égales* [...] *Nous n'avons pas la prétention de comparer nos modestes découvertes à celles de tous ces savants immortels ; mais c'est encore par l'observation de la suite de Fibonacci* $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$, *dans laquelle chaque terme est la somme des deux termes qui le précèdent, que nous avons rencontré une proposition nouvelle qui constitue la réciproque du théorème de Fermat. Nous en avons déduit un grand nombre de corollaires qui permettent de savoir si un nombre donné p de vingt ou trente chiffres est premier ou non, lorsque l'on connaît la décomposition en facteurs premiers de l'un des nombres* $(p \pm 1)$ *qui le comprennent*» [Lucas 1891a, p. XI-XII].

Il faut noter que bien des écrits de Lucas, à l'exception de l'article de l'*American Journal* et du *Traité*, ne contiennent aucune démonstration des propriétés annoncées. Pépin s'efforce de lever «*la forme ambiguë et indécise*» de certains théorèmes et le principal héritier de Lucas, l'américain D.H. Lehmer, formule en 1930 quelques remarques sur la qualité de ses démonstrations[63].

Pour faciliter les calculs numériques, Lucas dispose d'un *arithmomètre*, machine arithmétique effectuant les quatre opérations élémentaires, acquis grâce au soutien financier de l'AFAS. Au congrès de 1878 de l'association, Lucas préconise d'ailleurs l'utilisation de l'arithmomètre de Thomas pour

[63] «*Perhaps the most remarquable results of Lucas are included in a set of theorems concerning the prime or composite character of integers of certain forms. His conditions for primality are sufficient but not necessary*» [Lehmer 1930, section 5], repris dans [Lehmer 1981, 1, p. 34]. Ou encore :

«*A great deal of confusion exists in Lucas's writings about the exact enunciation and actual proofs of the tests for primality. Neverless, it is evident that Lucas was in possession of the facts needed to prove the sufficiency of these tests. The confusion arose from the fact that he was unable or unwilling to consider the necessity also*» [Lehmer 1935], repris dans [Lehmer 1981, 1, p. 86].

mener à bien les recherches dans le domaine de l'arithmétique supérieure et indique une amélioration à apporter à cet instrument pour son usage dans la théorie des congruences[64]. Lucas adapte également l'usage de l'échiquier au calcul binaire et au calcul des congruences ce qui le conduit à concevoir un instrument arithmétique nouveau.

ÉDOUARD LUCAS CONCEPTEUR D'INSTRUMENT

Édouard Lucas présente pour la première fois à Clermont-Ferrand, en 1876, le plan d'une «*machine arithmétique*» destinée à vérifier la primalité des nombres de Mersenne. Annoncé en quelques phrases dans les notes aux *Comptes rendus* de la même année[65], le plan de ce mécanisme apparaît à l'AFAS sous la forme de tableaux de calculs de résidus exprimés dans le système binaire [Lucas 1876d, p. 67]. Il est réédité en 1877 dans les *Comptes rendus* [Lucas 1877a, p. 441], dans le *Bulletino* de Boncompagni [Lucas 1877c, p. 158–159], ainsi qu'en 1878 dans l'*American Journal*

[64] On peut signaler que la *Société d'encouragement pour l'industrie nationale* contribue très largement, au cours du XIX^e^ siècle, à la promotion des machines à calculer à usage industriel et commercial, en particulier à celle de l'arithmomètre de Charles-Xavier Thomas de Colmar [Sebert 1879]. On doit noter que la médaille d'or de cette société est attribuée en 1880 à M. Thomas (de Bojano) pour les perfectionnements apportés à la machine de M. Thomas (de Colmar). Voir à ce sujet le [*Bulletin de la société d'encouragement*, 7 (1880), p. 403]. Entre 1802 et 1900, figurent également dans ce Bulletin des rapports sur les machines à calculer de Roth, Maurel et Jayet, Deprez, Péraux, Didelin, Bollée. Lucas y fait une communication en mars 1884 sur «*l'arithmétique figurative et ses applications*», Maurice d'Ocagne en février 1905 sur le «*calcul simplifié*».

[65] «*J'ai trouvé le plan d'un mécanisme assez simple, qui permettra de vérifier, automatiquement et en très peu de temps, les assertions du P. Mersenne, et de trouver de très-grands nombres premiers de* 80 *et même de* 100 *chiffres compris dans la forme* $a^n \pm 1$, *a étant égal à* 2, 3 *ou* 5. *La construction de ce mécanisme permet de calculer rapidement, dans le système binaire de la numération, les résidus* [...] *par rapport au nombre dont on cherche la décomposition en facteurs premiers et repose, d'une part, sur les théorèmes qui précèdent, et d'autre part sur les lois mathématiques du tissage*» [Lucas 1876b, p. 1305].

Et encore : «*Nous allons exposer une méthode nouvelle qui permet de reconnaître les nombres premiers très-grands, et de décomposer en leurs facteurs des nombres N très-grands, lorsque l'on connaît à l'avance la décomposition en ses facteurs premiers du nombre* $N \pm 1$. *Cette méthode a reçu l'approbation de MM. Genocchi et Tchebichef.*» «*J'ai conçu, en suivant cette voie, le plan d'un mécanisme qui permettrait de décider du mode de composition de ces nombres, et de trouver des nombres premiers ayant mille chiffres dans le système décimal et même beaucoup plus*» [Lucas 1876d, p. 62 et 68].

[Lucas 1878a, p. 306–308]. Même si l'auteur ne fournit que le principe mathématique de ce mécanisme, il manifeste par ces rééditions successives un intérêt qui ne se dément pas pour l'instrumentation et les applications «*pratiques*» de la science.

«*Le plus grand nombre premier que nous connoissions est sans doute* $2^{31} - 1 = 2147483647$*, que Fermat a déjà assuré être premier, et moi je l'ai prouvé aussi ; car* [...] *j'ai examiné tous les nombres premiers* [...] *jusqu'à* 46339*, dont aucun ne s'est trouvé diviseur*» annonce Euler [1772, p. 335–337]. Le propos est confirmé par Legendre qui écrit encore en 1830, dans la troisième édition de son traité de *Théorie des nombres*, que «*le nombre* $2^{31} - 1$ *est un nombre premier. C'est le plus grand de ceux qui aient été vérifiés jusqu'à présent*» [Legendre 1830, t. 1, p. 229].

Lucas se propose non seulement de vérifier ces assertions mais d'aller bien au-delà, grâce aux théorèmes qui lui permettent de savoir si un nombre est premier ou composé, sans avoir recours à la table des nombres premiers[66]. L'objectif de l'auteur est d'automatiser le calcul de la suite numérique $w_1 = 3$, $w_2 = 7, \ldots, w_k = w_{k-1}^2 - 2$ utilisée dans son test. En numération décimale, un calcul de ce type devient rapidement impraticable pour de grands nombres. Lucas le simplifie dans $\mathbb{Z}_p$ (p désigne le nombre à tester) en utilisant l'écriture binaire des nombres.

La méthode mêlant ces deux aspects (écriture binaire et calcul par congruences) est présentée de manière imagée dans la publication bolognaise de 1877. Pour effectuer des calculs dans $\mathbb{Z}_p$ avec $p = 2^7 - 1$, Lucas utilise un échiquier à 7 cases. Puisque l'on peut écrire $2^7 \equiv 1$, $2^8 \equiv 2$, $2^9 \equiv 2^2$, etc., la longueur des nombres écrits ne dépasse pas 7 chiffres. De plus multiplier par 2 un nombre écrit dans le système binaire revient ici à permuter circulairement les sept chiffres 0 et 1 qui figurent dans ce nombre[67].

---

[66] « *C'est à l'aide de ces théorèmes que je pense avoir démontré que le nombre* $2^{127} - 1$ *est premier. Ce nombre contient trente-neuf chiffres, tandis que le plus grand nombre premier connu actuellement n'en contient que dix. Ce nombre est, d'après Euler, égal à* $2^{31} - 1$ » [Lucas 1876a, p. 167].

[67] « *Nous remarquerons d'abord que la multiplication de deux nombres écrits dans le système binaire, c'est-à-dire, avec les deux chiffres* 0 *et* 1 *seulement, se fait par le simple déplacement longitudinal du multiplicande. D'autre part, il est clair que le reste de la division de* 2^m *par* $2^n - 1$ *est égal à* 2^r*, r désignant le reste de la division de m par n*» [Lucas 1877c, p. 155].

L'écriture binaire de 47 étant 0101111, celle de $2 \cdot 47$ est 1011110, celle de $2^2 \cdot 47$ est 0111101, (mod. $2^7 - 1$). D'une manière générale, si $p = 2^n - 1$, de l'écriture

«*Prenons pour l'essai de* 2^7-1*, un échiquier de sept cases de côté* [...] *la multiplication de* 47 *par* 47 *se fera de la façon suivante*» :

	2^6	2^5	2^4	2^3	2^2	2^1	2^0
$1\cdot 47$	0	1	0	1	1	1	1
$2\cdot 47$	1	0	1	1	1	1	0
$2^2\cdot 47$	0	1	1	1	1	0	1
$2^3\cdot 47$	1	1	1	1	0	1	0
$2^5\cdot 47$	1	1	0	1	0	1	1
47^2	0	1	1	0	0	1	0

L'addition finale, effectuée dans le système binaire, en respectant les règles d'écriture des nombres modulo $p=2^7-1$, s'obtient également sur l'échiquier :

«*On enlève ensuite deux pions de chaque colonne pour en reporter un dans la colonne à gauche, et dans la première à droite, lorsqu'on arrive à la dernière. Avec un peu d'exercice, on parvient assez rapidement à exécuter cette manœuvre*» [Lucas 1877c, p. 156].

Selon ce double principe de calcul par congruences pour le module $2^{31}-1$, et d'écriture des restes dans le système binaire de la numération, Lucas vérifie la primalité du nombre $2^{31}-1$. Son test consiste à montrer que le trentième terme de la suite des nombres w_k est nul, aucun autre n'étant nul avant ce rang-là. Dans son intervention au Congrès de 1876 de l'AFAS [Lucas 1876d, p. 67], figure sur un échiquier comportant 30 cases le calcul de $w_{26}=v_{2^{26}}$ à partir du carré du terme précédent w_{25}, ainsi que le tableau de tous les nombres w_k, de $k=0$ à $k=30$[68]. Dans [Lucas 1878a, p. 306], apparaît la conclusion de l'auteur :«*la dernière ligne, entièrement composée de zéros, nous montre que* $2^{31}-1$ *est premier*»[69].

binaire de a dans $\mathbb{Z}_p$ on déduit de manière «*automatique*» celle de $2a$, 2^2a, etc. : $a=a_{n-1}a_{n-2}\cdots a_1a_0$, $2a=a_{n-2}a_{n-3}\cdots a_1a_0a_{n-1}$, $2^2a=a_{n-3}\cdots a_1a_0a_{n-1}a_{n-2}$.

[68] Ces tableaux figurent également dans [Lucas 1877c, p. 158–159] et dans [Lucas 1878a, p. 306–307]. On trouve le diagramme de $2^{19}-1$ dans [Lucas 1877a, p.441] et dans [Lucas 1878a, p. 308].

[69] Lucas ajoute : « *On pourrait ainsi construire les diagrammes des nombres premiers de la forme* $2^{4q+3}-1$*. Nous donnons aussi celui du nombre* $2^{19}-1$*; nous espérons donner ultérieurement ceux des nombres* $2^{67}-1$ *et* $2^{127}-1$ [...] *Lorsque le nombre essayé n'est pas premier, nous avons vu qu'on ne trouvera aucun résidu nul*» [Lucas 1878a, p. 307–308].

Dans ces tableaux, où «*les carrés noirs représentent les unités des différents ordres du système binaire, et les carrés blancs représentent les zéros*» [Lucas 1877c, p. 160] ne peut-on voir l'ébauche du piano arithmétique dont Genaille présente le projet en 1891 à l'AFAS ? La dernière ligne du tableau des w_k est entièrement composée de carrés blancs, les lignes antérieures présentant toutes des carrés noirs mêlés aux blancs : la primalité du nombre testé est ainsi établie. Si un mécanisme effectuant automatiquement les opérations ci-dessus voit le jour, son réalisateur n'est en effet pas l'arithméticien mais l'ingénieur civil Henri Genaille, contemporain de Lucas et membre actif de l'AFAS. Il est connu pour ses réglettes multiplicatrices inspirées des bâtons de Neper et pour divers calculateurs financés en partie par l'association[70]. C'est en se réclamant de l'héritage de Lucas que Genaille conçoit pour le congrès de 1891 (année de la mort de l'arithméticien) un «*piano arithmétique pour la vérification des grands nombres premiers*» dont le fonctionnement est décrit en ces termes :

«*Le piano arithmétique permet de donner une suite pratique à la méthode formulée par M. E. Lucas, au Congrès de Clermont-Ferrand, pour la vérification des grands nombres premiers. Par la manœuvre simple de quelques chevilles, la vérification des nombres premiers de la forme* $2^n - 1$ *se trouve réduite dans la plus grande partie des cas à un travail de quelques heures. Cette machine, qui peut arriver à faire automatiquement des calculs de la plus grande importance, réalisera un jour la solution d'une machine à calculer faisant seule les opérations arithmétiques*» [Genaille 1891, p. 158].

On trouve dans l'*Encyclopédie des sciences mathématiques* une description analogue de l'instrument dans l'article de M. d'Ocagne et R. Mehmke intitulé «*Calculs numériques*» :

«*On doit à H. Genaille un "piano arithmétique" dont la partie esentielle est une règle à chevilles qui permet de reconnaître, parmi les nombres de la forme* $2^n - 1$ *inférieurs à un nombre donné, ceux qui sont premiers*»

[70] La présentation des réglettes et autres réalisations de l'ingénieur est faite par Lucas lui-même au congrès de 1884 : «*Pour tous les calculs spéciaux, de toute nature, il vous imaginera, d'une manière tellement rapide qu'il m'est souvent difficile de le suivre, des tableaux graphiques pour la solution des calculs proposés. En un mot, il a le génie des calculs pratiques*» [Lucas 1884a, p. 139].

[*Encyclopédie* t. 1, vol. 4, p. 271][71].

À ce jour, on n'a pas de trace de ce piano arithmétique. En tout état de cause, les congrès de l'AFAS apparaissent comme des lieux privilégiés ouverts à la présentation d'instruments à usage scientifique[72]. Ainsi au congrès de La Rochelle (1882), Pafnuti Tchebychef présente son propre arithmomètre à mouvement continu, qui utilise un système de trains épicycloïdaux et ressemble «*de loin à la cage d'un écureuil*» [Lucas 1891c, t. 3, p. 74]. Lucas œuvre pour que cette machine demeure en France et elle sera offerte par son auteur au Conservatoire national des arts et métiers [Jongmans et Butzer 1989]. Les conceptions de Charles Babbage parvenues en France par l'intermédiaire de L.F. Menabrea, trouvent naturellement un écho à l'AFAS : pour pallier aux innombrables erreurs qui entachent les tables numériques de l'époque, une mécanisation des opérations est jugée plus sûre. Une collection d'instruments et de machines à calculer, réunie par Édouard Lucas avec le concours financier de l'association, est ainsi léguée en 1888 par l'arithméticien au Conservatoire national des arts et métiers. Ultérieurement Leonardo Torres y Quevedo expose au congrès de Bordeaux (1895) les principes de son étonnante machine à équations, dont les éléments mécaniques sont baptisés «*arithmophores logarithmiques*».

[71] Une mention du «*piano arithmétique*» de Genaille pour tester les grands nombres premiers figure déjà dans l'article «*Numerisches Rechnen*» de R. Mehmke [*Encyklopädie* 1901, t. I, fasc. 6, p. 978 note 185].

[72] Voir [Décaillot 1997]. On peut remarquer que ce courant instrumentaliste occupe une place assez modeste à l'Académie des sciences. Dans les notes aux *Comptes rendus*, de 1870 au début du XX^{e} siècle, figurent quelques références à des machines à calculer et à des machines arithmétiques. La machine analytique de Charles Babbage y est décrite sommairement par L.F. Menabrea [1884] (notons qu'un mémoire sur ce sujet est publié dès 1842 à Genève par Menabrea [1842]) ; la machine à différences de Wiberg fait l'objet d'une description de Ch.-E. Delaunay dans les notes aux *Comptes rendus* en 1863. Léon Bollée [1889] présente sa multiplicatrice de conception tout à fait nouvelle en 1889 : elle est à multiplication directe, alors que toutes les mutiplicatrices depuis Leibniz effectuent la multiplication par additions répétées. L. Torres y Quevedo rédige notes et mémoire, entre 1895 et 1902, sur ses machines permettant d'obtenir les racines réelles et complexes des équations algébriques [Torres y Quevedo 1895], [Torres y Quevedo 1900], [Torres y Quevedo 1902]. G. Meslin [1900] intervient en 1900 à propos d'une machine à résoudre les équations au moyen d'une balance hydrostatique.

LA POSTÉRITÉ D'ÉDOUARD LUCAS

Le troisième volume de l'*Encyclopédie des sciences mathématiques*, consacré à la théorie des nombres, accorde, dans sa version allemande de 1900 (*Niedere Zahlentheorie*) aussi bien que dans sa traduction française de 1906, une place aux travaux d'Édouard Lucas. Dans le monumental ouvrage de Leonard-Eugene Dickson, *History of the Theory of Numbers*, publié à partir de 1919, Lucas apparaît pour ses travaux concernant la primalité des nombres de Mersenne et pour avoir établi la vraie réciproque du petit théorème de Fermat. Dickson n'omet pas de mentionner que l'arithméticien affirme avoir conçu «*le plan d'un mécanisme qui permet de décider presque instantanément si les assertions de Mersenne et Plana concernant la primalité de* $2^n - 1$ *pour certaines grandes valeurs de n sont exactes*» [Dickson, vol. 1, p. 22]. Près d'un chapitre du premier volume de l'ouvrage est consacré aux résultats de Lucas concernant les suites de Léonard de Pise et de Pell, ainsi qu'aux tests de primalité qui en découlent.

La filiation française de Lucas semble de bien faible ampleur. Nous avons mentionné Théophile Pépin, contemporain d'Édouard Lucas, qui approfondit sa démarche. Auguste Aubry, en 1913, effectue une longue synthèse des procédés de factorisation dus à Genocchi, Lucas et leurs successeurs ; Auguste Pellet en 1916 et Léon Pomey en 1920 publient de courtes notes sur des thèmes proches. L'héritier le plus actif de Lucas semble être en France l'arithméticien André Gérardin, membre actif de l'AFAS à partir de 1909. On lui doit de nombreuses publications, en particulier dans la revue *Sphinx-Œdipe* qu'il rédige et édite. Il intervient en 1913 au cinquième congrès international des mathématiciens sur les nouvelles machines algébriques et conçoit le plan d'une machine à congruences pour décomposer les nombres en leurs facteurs premiers, selon une idée proche de celle de Maurice Kraïtchik [1922, p. 43]. Cette machine est réalisée en 1920 par les frères Carissan ; redécouverte récemment, elle utilise des méthodes de criblage[73].

Par comparaison il faut souligner que Lucas est à l'origine d'une filiation anglo-américaine conséquente. L'importance du mémoire qu'il publie en 1878 dans l'*American Journal* contribue certainement à la pénétration de cette influence. Allan Cunningham réagit dès 1894 à la

[73] Voir [Morain, Shallit, Williams 1995] et [Morain, Shallit, Williams 1996].

publication des premiers tests concernant les nombres de Mersenne. Dans son long mémoire de 1913, Robert Daniel Carmichael généralise plusieurs théorèmes de Lucas et rectifie certaines de ses erreurs (par exemple dans la démonstration du résultat de Genocchi). Carmichael obtient des conditions nécessaires et suffisantes de primalité d'un nombre en utilisant le polynôme cyclotomique qui lui est associé, et ses résultats généralisent ceux de Pépin[74]. Alfred Edward Western revient en 1932 sur les résultats énoncés par Lucas ou Pépin, dont il juge les démonstrations incomplètes, et joint la liste des nombres de Mersenne examinés grâce à leurs tests.

L'héritier principal de Lucas demeure Derrick Henry Lehmer qui, entre 1927 et 1932, parachève son œuvre en perfectionnant ses tests de primalité relatifs aux nombres de Mersenne, au point que les découvertes actuelles de très grands nombres premiers, utiles par exemple en cryptographie, sont toujours effectuées grâce au test dit de Lucas-Lehmer, [Cohen 1995] et [Cohen 1996].

La réciproque du théorème de Fermat reçoit tout d'abord une simplification sensible en 1927 lorsque D.H. Lehmer établit le résultat suivant : a et n étant premiers entre eux,

«*Si* $a^{n-1} \equiv 1$ (*mod. n*) *et si* $a^{(n-1)/d} \not\equiv 1$ (*mod. n*)*, pour tout diviseur premier d de* $n-1$*, alors n est premier*» [Lehmer 1981, vol. 1, p. 70].

L'application de ce résultat peut demander beaucoup moins de vérifications que celui de Lucas. Ainsi le nombre de Fermat $2^{2^4}+1 = 65537$ peut être déclaré premier en deux étapes seulement.

Après les travaux de Lucas et Pépin, la nécessité de démonstrations rigoureuses s'impose et Lehmer contribue à la clarification de leurs critères en 1930. Son théorème met en jeu une suite dont le terme général est $u_n = (a^n - b^n)/(a-b)$ (a et b désignent les racines distinctes d'une équation du second degré à coefficients entiers et premiers entre eux) :

Étant donné un entier N, les nombres q_i désignent les facteurs premiers de $N \pm 1$, et l'on pose $m_i = (N \pm 1)/q_i$. Si $u_{N\pm1} \equiv 0$ (mod. N) et si

[74] Mais il doit avouer : «*In general the above theorems are not convenient in practice for the verification that a given number p is prime unless p is of special form*» [Carmichael 1913, p. 66]. L'application des tests de Carmichael, facile pour les nombres de Fermat, est moins aisée pour ceux de Mersenne. Donnant sur ce point raison à Lucas, Lehmer fait remarquer que, d'un point de vue pratique, ce dernier type de résultat demeure en général inapplicable car il dépend d'un couple de nombres auxiliaires, pour la détermination duquel aucune méthode n'est fournie.

$u_{m_i} \not\equiv 0 \pmod{N}$ pour tous les nombres m_i, alors le nombre N est premier [Lehmer 1981, vol. 1, p. 34–37].

Le nombre de vérifications à effectuer peut être ici beaucoup moins élevé que par le critère de Lucas. Néanmoins le résultat général demeure une condition suffisante de primalité. Pour les nombres de Mersenne cependant, Lehmer élabore un critère nécessaire et suffisant de primalité. Pousuivant la réflexion de Pépin, il s'intéresse à la détermination du premier terme des suites récurrentes (du type $s_{k+1} = s_k^2 - 2$) qui peuvent conduire à un critère de cette nature. Lehmer montre que le problème admet une infinité de réponses et une méthode de construction de ce premier élément est détaillée : il peut être 4, ou 10, ou 52 (déjà proposé par Pépin[75]), ou 724... L'auteur parvient à l'énoncé suivant :

« *Le nombre $N = 2^n - 1$, où n est un nombre premier impair, est premier si et seulement si N divise le $(n-1)$-ième terme de la série : $s_1 = 4$, $s_2 = 14$, $s_3 = 194, \ldots, s_k, \ldots$ où $s_k = s_{k-1}^2 - 2$* » [Lehmer 1981, vol. 1, p. 86]

Lehmer publie les preuves complètes de ses résultats qui étonnent par la simplicité des méthodes utilisées. Leur démonstration est faite également par Western en 1932 grâce à la théorie des nombres algébriques. Une synthèse des résultats de ces auteurs est effectuée dans [Hardy et Wright 1938].

Sur l'exemple décisif des tests de primalité, l'influence de Lucas apparaît beaucoup plus faible en France qu'à l'étranger, principalement aux États Unis. Elle amène à s'interroger sur les fondements de ce développement inégal, ainsi que sur le rôle des applications dans le milieu savant français de la fin du XIX$^{\text{e}}$ siècle. On peut remarquer que des études récentes concernant la primalité et la décomposition des nombres utilisent la théorie des fonctions elliptiques, et les méthodes de Lucas ou Pépin n'y sont pas étrangères [Koblitz 1987]. Pour sa part, la décomposition des polynômes cyclotomiques dans un corps fini a trouvé d'importantes applications dans l'établissement de codes correcteurs [Demazure 1997].

[75] Pépin propose, pour tester le nombre $q = 2^7 - 1$, de choisir une suite de premier terme 52 [Pépin 1878, p. 309–310].

ANNEXE

Tableaux extraits de l'intervention d'Édouard Lucas [1876d, p. 67].

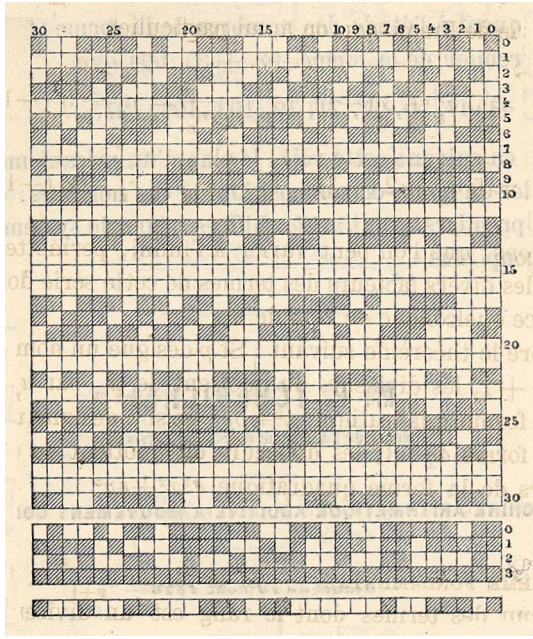

Figure 1. Calcul dans le système binaire, suivant le module $2^{51}-1$*, du résidu du terme* v *de rang* 2^{26}*, à l'aide de celui du terme de rang* 2^{25}*.*

BIBLIOGRAPHIE

Association française pour l'avancement des sciences
[AFAS] *Congrès*, 1 à 43, Paris 1872–1914.

Aubry (Auguste)
[1913] Sur divers procédés de factorisation, *L'Enseignement mathématique*, 15 (1913), p. 202–230.

Bachmann (Paul)
[1900] Niedere Zahlentheorie, [*Encyklopädie*], I, Heft 5, p. 555–581.

Bachmann (Paul) et Maillet (Edmond)
[1906] Propositions élémentaires de la théorie des nombres, [*Encyclopédie*], 3, fasc. 1, p. 1–75.

Bertrand (Joseph)
[1845] Mémoire sur le nombre de valeurs que peut prendre une fonction quand on permute les lettres qu'elle renferme, *Journal de l'École royale polytechnique*, 18 (1845), cahier 30, p. 123–140.

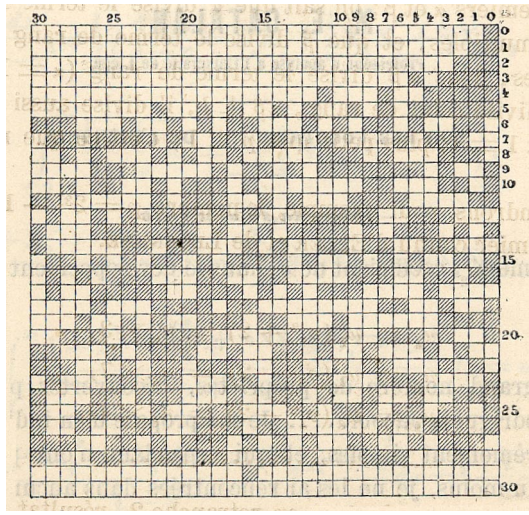

Figure 2. Tableau des résidus des termes v de rangs $1, 2, 2^2, 2^3, \ldots, 2^{30}$*, suivant le module* $2^{31} - 1$*, et faisant voir que ce module est un nombre premier.*

Bollée (Léon)
[1889] Sur une nouvelle machine à calculer, *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, 109 (1889), p. 737–739.

Borel (Émile)
[1953] *Les nombres premiers*, Paris : Presses Universitaires de France, Que-sais-je ?, 1953.

Cahen (Eugène)
[1900] *Éléments de la théorie des nombres*, Paris : Gauthier-Villars, 1900.

Carmichael (Robert Daniel)
[1913–14] On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Annals of Mathematics*, 2^e s., 15 (1913–14), p. 30–79.

Chabert (Jean–Luc), dir.
[1994] *Histoire d'algorithmes, du caillou à la puce*, Paris : Belin 1994.

Cohen (Henri)
[1995] Les nombres premiers, *La Recherche*, août 1995, p. 760–765.
[1996] Le dernier des premiers, *La Recherche*, octobre 1996, p. 16.

Combette (Eugène Charles)
[1892] Notice nécrologique d'Édouard Lucas, *Annuaire de l'association des anciens élèves de l'École normale*, 1892, p. 57–59.

Cunningham (Allan)
[1894] On Mersenne's numbers, *British Association Reports*, 1894, p. 563–564.
[1895–96] Note by the Lieut. Col. Allan Cunningham, R.E., *Proceedings of the London Mathematical Society*, 27 (1895–96), p. 53– 54.

[1899] On Fermat's numbers, *British Assoc. Reports*, 1899, p. 653–654.

[1912–13] On Mersenne's numbers, *British Assoc. Reports*, 1912–13, p. 406.

Décaillot (Anne-Marie)

[1997] L'AFAS : la promotion de l'instrument, dans [GHDSO 1997], p. 63–72.

Delaunay (Charles Eugène)

[1863] Rapport sur la machine à calculer présentée par M. Wiberg, *C. R. Acad. sci. Paris*, 56 (1863), p. 330–339.

Demazure (Michel)

[1997] *Cours d'algèbre. Primalité, divisibilité, codes*, Paris : Cassini 1997.

Dickson (Leonard Eugene)

[1919–23] *History of the Theory of Numbers*, 3 vols, Washington : Carnegie Institut of Washington, 1919–23 (réimpression New York : Chelsea, 1952).

Echeverria (Javier)

[1992] Observations, problems and conjectures in number theory. The history of the prime number theorem, in : Echeverria (J.), Ibarra (I.) & Mormann (I.), eds., *The Space of Mathematics*, Berlin & New–York : de Gruyter, 1992, p. 230–252.

[1996] Empirical methods in mathematics. A case study : Goldbach's conjecture, in Munevar (G.), ed., *Spanish Studies in the Philosophy of Science*, Dordrecht : Kluwer, 1996, p. 19–55.

Encyklopädie der mathematischen wissenschaften mit einschluss ihrer anwendungen

[*Encyklopädie*] t. I–VII, Leipzig 1898–1907.

Encyclopédie des sciences mathématiques pures et appliquées

[*Encyclopédie*] Édition française rédigée et publiée d'après l'édition allemande, t. I–VII, Paris : Gauthier–Villars 1904–1916 ; réédition Gabay 1991.

Euler (Leonhard)

[*Opera*] *Leonhardi Euleri Opera omnia*, 1e série, 27 vol., Leipzig : Teubner 1911–1956

[1748] De seriebus ex evolutione factorum ortis, *Introductio in analysin infinitorum*, t. 1, ch. XV, Lausanne : éd. Bousquet, 1748 ; *Opera* (I), 8, p. 284–312.

[1750] Theoremata circa divisores numerorum, *Novi commentarii academiae scientiarum Petropolitanae*, 1 (1747–48), 1750, p. 20–48 ; *Opera* (I), 2, p. 62–85.

[1769] Quomodo numeri praemagni sint explorandi utrum sint primi necne, *Novi com. acad. sci. Petropolitanae*, 13 (1768), 1769, p. 67–88 ; *Opera* (II), 3, p. 112–130.

[1772] Extrait d'une lettre de M. Euler le père à M. Bernoulli concernant le Mémoire imprimé parmi ceux de 1771, p. 318, *Nouveaux mémoires de l'académie des sciences de Berlin* 1772, 1774, partie *Histoire*, p. 35–36 ; *Opera* (I), 2, p. 335–337.

[1774] Demonstrationes circa residua ex divisiones potestatum per numeros primos resultantia, *Novi com. acad. sci. Petropolitanae*, 18 (1773), 1774, p. 85–135 ; *Opera* (I), 2, p. 240–281.

[1783] Miscellanea analytica. Theorema a Cl. Waring sine demonstrationes propositum, *Opuscula Analytica*, t. 1, Saint-Pétersbourg, 1783, p. 329–344 ; *Opera* (I), 3, p. 91–104.

[1785] De summa seriei ex numeris primis formatae. . . , *Opuscula Analytica*, t. 2, Saint-Pétersbourg 1775, 1785, p. 240–256 ; *Opera* (I), 3, p. 146–162.

FENSTER (Della Dumbaugh)

[1998] Leonard Eugene Dickson and his work in the arithmetics of algebras, *Archive for History of Exact Sciences*, 52 (1998), p. 119–159.

GAUSS (Carl Friedrich)

[1801] *Disquisitiones Arithmeticae*, Leipzig 1801,

[1807] *Recherches arithmétiques*, trad. fr. de [Gauss 1801], Paris : Poullet-Delisle, 1807 (rééd. Blanchard 1953 et Gabay 1989).

GENAILLE (Henri)

[1891] Piano arithmétique pour la vérification des grands nombres premiers, AFAS, 20 (1891), t. 1, p. 159.

GENOCCHI (Angelo)

[1868–69] Intorno ad alcune forme di numeri primi, *Annali di matematica pura ed applicata*, 2^{e} s., 2 (1868–69), p. 256–267.

[1875–76$_{a}$] Intorno a tre problemi aritmetici di Pietro Fermat, *Atti della reale Accademia delle science di Torino*, 11 (1875–76), p. 811–829.

[1875–76$_{b}$] Cenni di ricerce interno ai numeri primi, *Ibid.*, p. 924–927.

[1884] Sur les diviseurs de certains polynômes et l'existence de certains nombres premiers, *C. R. Acad. sci. Paris*, 98 (1884), p. 411–413.

GÉRARDIN (André)

[1909$_{a}$] Résolution en entiers positifs de $x^n + y^n + z^n = u^n + v^n$, AFAS, 38 (1909), t. 2, p. 143–145.

[1909$_{b}$] Décomposition des grands nombres, AFAS, 38 (1909), t. 2, p. 145–156.

[1912] Rapport sur diverses méthodes de solutions employées en théorie pour la décomposition des nombres en facteurs, AFAS, 41 (1912), t. 2, p. 54–57.

[1912–13] Sur une nouvelle machine algébrique, *British Assoc. Reports*, 1912–13, p. 405–406.

[1913] Sur quelques nouvelles machines algébriques, *Proceedings of the Fifth International Congress of Mathematicians, Cambridge*, t. 2, p. 572–573.

[1914] Arithmétique supérieure, machines à calculs entiers, applications inédites, AFAS, 43 (1914), t. 2, p. 26–28.

[1916] Solutions de questions proposées (n^{o} 2121), *Nouvelles annales de mathématiques*, 4^{e} s., 16 (1916), p. 361–367.

[1932] Factorisations quadratiques et primalité, *Sphinx-Œdipe*, Nancy, août 1932, p. 3–95.

GROUPE D'HISTOIRE ET DE DIFFUSION DES SCIENCES D'ORSAY (GHDSO)

[1997] Une entreprise de diffusion des sciences sous la III^{e} République : l'Association française pour l'avancement des sciences (AFAS) (1872–1914), dans Centre interdisciplinaire de l'étude des évolutions des idées scientifiques et techniques, éd., *Nécessité et pièges de la vulgarisation, Orsay* : Paris Onze-Éditions, 1997, p. 41–77.

GISPERT (Hélène)

[1991] La France Mathématique, La Société Mathématique de France (1872–1914), *Cahiers d'histoire et de philosophie des sciences*, 34, Paris : Société française d'Histoire des sciences et des techniques, Société mathématique de France, 1991.

GOHIERRE DE LONGCHAMPS (Gaston)

[1877] Sur la décomposition en facteurs premiers des nombres $2^n \pm 1$, *C. R. Acad. Sci. Paris*, 85 (1877), p. 950–952.

Goldstein (Catherine)
[1994] La théorie des nombres dans les *Notes aux Comptes Rendus de l'Académie des sciences* (1870–1914) : un premier examen, *Rivista di storia della scienza*, 2e s., 2 (1994), p. 137–160.
Hadamard (Jacques)
[1892] Détermination du nombre de nombres premiers inférieurs à une quantité donnée, *C. R. Acad. sci. Paris*, 115 (1892), p. 1120–22.
[1896] Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences, *Bull. Soc. math. France*, 1896, p. 199-220.
Hardy (Godefrey Harold) et Wright (E.M.)
[1938] *An Introduction to the Theory of Numbers*, Oxford : Oxford University Press, 1938.
Harkin (Duncan)
[1957] On the mathematical work of François-Édouard-Anatole Lucas, *L'Enseignement mathématique*, 2e s., 3 (1957), p. 276–288.
Hulin-Jung (Nicole)
[1989] *L'organisation de l'enseignement des sciences : la voie ouverte par le Second Empire*, Paris : C.T.H.S., 1989.
Itard (Jean)
[1967] *Arithmétique et théorie des nombres*, Paris : Presses Universitaires de France, Que-sais-je ?, 1967.
[1969] *Les nombres premiers*, Paris : Presses Universitaires de France, Que-sais-je ?, 1969.
Jacob (L.)
[1911] *Le calcul mécanique. Appareils arithmétiques et algébriques. Intégrateurs*, Paris : Octave Douin, 1911.
Jongmans (François) et Butzer (Paul)
[1989] P. L. Chebyshev (1821–1894) and his contacts with western european scientists, *Historia mathematica*, 16 (1989), p. 46–68.
Jongmans (François)
[1996] *Eugène Catalan, Géomètre sans patrie, Républicain sans république*, Mons : Société belge des professeurs de mathématique d'expression française, 1996.
Koblitz (Neal)
[1987] *A Course in Number Theory and Cryptography*, New York, Berlin, Paris etc. : Springer-Verlag, 1987.
Kraïtchik (Maurice)
[1922–26] *Théorie des nombres*, 2 vols., Paris : Gauthiers-Villars, 1922–26.
Lagrange (Joseph Louis)
[*Œuvres*] *Œuvres de Lagrange*, J.-A. Serret et G. Darboux, éd., 14 vol., Paris : Gauthier-Villars, 1867–1892
[1766–69] Solution d'un problème d'arithmétique, *Miscellanea taurinensia*, 4 (1766–69) ; *Œuvres* 1, p. 671–731.
[1771] Démonstration d'un théorème nouveau concernant les nombres premiers, *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin*, 2, p. 125–137 ; *Œuvres* 3, p. 425–438.
[1775] Recherches d'arithmétique, *Ibid.* 1773 et 1775 ; *Œuvres* 3, p. 695–795.
Laisant (Charles-Ange)
[1879] Discours d'ouverture, AFAS, 8 (1879), p. 61–116.
[1887a] Notice historique sur les travaux des première et deuxième sections de 1879 à 1886 inclusivement, AFAS, 16 (1887), t. 1, p. 163.

[1887b] Quelques applications arithmétiques de la géométrie des quinconces, AFAS, 16 (1887), t. 2, p. 218–235.

[1891] Note bibliographique relative à l'ouvrage *Théorie des nombres* d'Édouard Lucas, *Journal de mathématiques spéciales*, 3e s., 5 (1891), p. 278–280.

[1904] Le rôle social de la science, AFAS, 33 (1904), t. 1, p. 160–179.

Lambert (Jean Henri)

[1769] Adnotata quaedam de numeris eorumque anatomia, *Nova acta eruditorum*, 1769, p. 107–128 ; *Opera Mathematica* 2, Speiser (A.), éd., 1948, p. 198–213.

Lamé (Gabriel)

[1844] Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers, *C.R. Acad. sci. Paris*, 19 (1844), p. 867–870.

Legendre (Adrien-Marie)

[1785] Recherches d'analyse indéterminée, *Mémoires de l'Académie royale des sciences*, 1785, p. 465–559.

[1798] *Essai sur la théorie des nombres*, Paris, an VI.

[1830] *Théorie des nombres*, 3e éd., Paris : Firmin Didot, 1830 (rééd. Blanchard 1955).

Lehmer (Derrick Henry)

[1927] Test for primality by the converse of Fermat's theorem, *Bulletin of the American Mathematical Society*, 33 (1927), p. 327–340.

[1930] An extended theory of Lucas's functions, *Annals of Mathematics*, 31 (1930), p. 419–448.

[1935] On Lucas's test for the primality of Mersenne's numbers, *Journal of the London Mathematical Society*, 10 (1935), p. 162–165.

[1981] *Selected papers of D. H. Lehmer*, 3 vols, Winnipeg : Charles Babbage Research Center, 1981.

Lejeune-Dirichlet (Gustav Peter)

[1837] Jede arithmetische Progression..., *Bericht über die zur Bekanntmachung geeigneten Verhandlungen der Königl. Preuss. Akademie der Wissenschaften zu Berlin*, lu le 27 juillet 1837, p. 108–111.

Lucas (Édouard)

[1867] *Application de l'arithmétique à la construction de l'armure des satins réguliers*, Paris : G. Retaux, 1867.

[1873] *Recherches sur l'analyse indéterminée et l'arithmétique de Diophante*, Moulins : Desrosiers, 1873 ; rééd. Paris : Blanchard, 1961.

[1875] Sur la décomposition des nombres en facteurs premiers, *Nouvelles annales de mathématiques*, 2e s., 14 (1875), p. 523–525.

[1875–76] Sur la théorie des nombres premiers, *Atti della reale Accademia delle science di Torino*, 11 (1875–76), p. 928–937.

[1876a] Note sur l'application des séries récurrentes à la recherche de la loi de distribution des nombres premiers, *C. R. Acad. sci. Paris*, 82 (1876), p. 165–167.

[1876b] Sur les rapports qui existent entre la théorie des nombres et le calcul intégral, *C. R. Acad. sci. Paris*, 82 (1876), p. 1303–1305.

[1876c] Nouveaux théorèmes d'arithmétique supérieure, *C. R. Acad. sci. Paris*, 83 (1876), p. 1286–1288.

[1876d] Sur la recherche des grands nombres premiers, AFAS, 5 (1876), p. 61–68.

[1877a] Sur l'extension du théorème de Fermat généralisé, et du *Canon arithmeticus*, *C. R. Acad. sci. Paris*, 84 (1877), p. 439–442.

[1877b] Sur la division de la circonférence en parties égales, *C. R. Acad. sci. Paris*, 85 (1877), p. 136–139.
[1877c] Recherches sur plusieurs ouvrages de Léonard de Pise et sur diverses questions d'arithmétique supérieure, *Bulletino di bibliografia e di storia delle scienze matematiche e fisiche*, 10 (1877), p. 129–193 et p. 239–293.
[1877d] Théorie nouvelle des nombres de Bernoulli et d'Euler, *Annali di matematica pura ed applicata*, 2e s., t. 8 (1877), p. 56–76.
[1877e] Formules fondamentales de géométrie tricirculaire et tétrasphérique, *Ibid.*, p. 187–192.
[1877f] Considérations nouvelles sur la théorie des nombres premiers et de la division géométrique de la circonférence en parties égales, AFAS, 6 (1877), p. 159–167.
[1877–78] Théorèmes d'arithmétique, *Atti della reale Accademia delle science di Torin*, 13 (1877–78), p. 271–284.
[1878a] Théorie des fonctions numériques simplement périodiques, *American Journal of Mathematics pure and applied*, 1 (1878), p. 184–240 et p. 289–321.
[1878b] Sur la série récurrente de Fermat, *Bulletino di bibliografia e di storia delle scienze matematiche e fisiche*, 11 (1878), p. 783–798.
[1878c] Sur l'emploi de l'arithmomètre de Thomas dans l'arithmétique supérieure, AFAS, 7 (1878), p. 94–95.
[1880] Sur les fonctions cyclotomiques, *C. R. Acad. sci. Paris*, 90 (1880), p. 855–856.
[1884a] Le calcul et les machines à calculer, AFAS, 13 (1884), p. 111–141.
[1884b] L'arithmétique figurative et ses applications, *Bulletin de la société d'encouragement pour l'industrie nationale*, 3e s., 11 (1884), p. 210.
[1886] Sur l'emploi des critériums cubiques, biquadratiques et octiques suivant un module premier, AFAS, 15 (1886), t. 2, p. 101–103.
[1888] Sur un théorème de Cauchy, AFAS, 17 (1888), t. 2, p. 29–31.
[1890] Sur la loi de réciprocité des résidus quadratiques, *Bulletin de l'Académie des sciences de Saint-Pétersbourg*, 33 (1890), p. 495–496.
[1891a] *Théorie des nombres*, t. 1, Paris 1891 ; rééd. Paris : Blanchard 1961 et Gabay 1991.
[1891b] Questions proposées à la discussion des première et deuxième sections, AFAS, 20 (1891), t. 1, p. 149–152.
[1891c] *Récréations mathématiques*, 4 vol., Paris 1891 ; rééd. Paris : Blanchard 1960.
[1895] *L'arithmétique amusante*, Paris 1895 ; rééd. Paris : Blanchard 1974.
[1911] Les principes fondamentaux de la géométrie des tissus, AFAS, 40 (1911), t. 2, p. 72–88 (mémoire extrait de l'*Ingeniere civile*, Turin 1880 et trad. de l'italien par A. Aubry et A. Gérardin).

Menabrea (Luigi Federico)
[1842] Notions sur la machine analytique de M. Charles Babbage, *Bibliothèque universelle de Genève*, 41 (1842), p. 352–376.
[1884] Sur la machine analytique de Charles Babbage, *C. R. Acad. sci. Paris 99*, (1884), p. 179–182.

Meslin (Georges)
[1900] Sur une machine à résoudre les équations, *C. R. Acad. sci. Paris*, 130 (1900), p. 888–890.

Morain (F.), Shallit (J.O.) et Williams (H.C.)
[1995] Discovery of a lost factoring machine, *The Mathematical Intelligencer* 17 (1995), p. 41–47.

[1996] La machine à congruences, *La revue des arts et métiers*, 14 (1996), p. 14–19.

Nicolas (Jean-Louis)

[1984] Tests de primalité, *Expositiones mathematicae*, 2 (1984), p. 223–234.

Ocagne (Maurice d')

[1893] *Le calcul simplifié par les procédés mécaniques et graphiques*, Paris : Gauthier-Villars, 1893.

Pellet (Auguste)

[1916] Réponse à une question de C.A. Laisant (n° 4452), *L'intermédiaire des mathématiciens*, 23 (1916), p. 64–67.

Pépin (Théophile)

[1877] Sur la formule $2^{2^n}+1$, *C. R. Acad. sci. Paris*, 85 (1877), p. 329–331.

[1878] Sur la formule 2^n-1, *C. R. Acad. sci. Paris*, 86 (1878), p. 307–310.

Pierce (Tracy A.)

[1916–17] The numerical factors of the arithmetic forms $\prod_{i=1}^{m}(1\pm\alpha_i^m)$, *Annals of Mathematics*, 1916–17, (2), 18, p. 53–64.

Pomey (Léon)

[1920] Sur les nombres de Fermat, *C. R. Acad. sci. Paris*, 170 (1920), p. 100–101.

Samuel (Pierre)

[1967] *Théorie algébrique des nombres*, Paris : Hermann, 1967.

Sebert Colonel

[1879] Rapport sur l'arithmomètre inventé par Thomas (de Colmar) et perfectionné par Thomas (de Bojano), *Bulletin de la société d'encouragement pour l'industrie nationale*, 6 (août 1879), p. 393–411.

Serres (Michel), dir.

[1989] *Éléments d'histoire des sciences*, Paris : Bordas, 1989.

Sylvester (James Joseph)

[1880a] Sur les diviseurs des fonctions cyclotomiques, *C. R. Acad. sci. Paris*, 90 (1880), p. 287–289 et p. 345–347.

[1880b] Sur la loi de réciprocité dans la théorie des nombres, *C. R. Acad. sci. Paris*, 90 (1880), p. 1053–1057 et p. 1104–1106.

Tannery (Jules)

[1895] *Introduction à l'étude de la théorie des nombres et de l'algèbre supérieure*, (notes rédigées par Émile Borel et Jules Drach), Paris : Nony, 1895.

Tchebychef ou Chebyshev (Pafnuti Lvovich)

[1850] Mémoire sur les nombres premiers (présenté à l'Académie impériale de Saint–Pétersbourg en 1850), *Journal de mathématiques pures et appliquées*, 17 (1852), p. 366–390.

Torres y Quevedo (Leonardo)

[1895] Sur les machines algébriques, *C. R. Acad. sci. Paris*, 121 (1895), p. 245–248.

[1900] Sur les machines à calculer, *C. R. Acad. sci. Paris*, 130 (1900), p. 472–474 et p. 874–876 .

[1902] Machines à calculer, *Mémoires présentés par divers savants à l'académie des sciences de l'Institut de France*, 2e s., t. 32, n° 9, p. 1–20.

Tournès (Dominique)

[1998] L'origine des méthodes multipas pour l'intégration numérique des équations différentielles ordinaires, *Revue d'histoire des mathématiques*, 4 (1998), p. 5–72.

Waring (Edward)

[1770] *Meditationes algebricae*, Cambridge, 1770.

Warusfel (André)
[1971] *Structures algébriques finies*, Paris : Hachette Université, 1971.
Weil (André)
[1974] Essais historiques sur la théorie des nombres, *L'Enseignement mathématique*, 20 (1974), p. 87–110, 215–222, 247–263.
[1983] *Number theory. An approach through history : from Hammurapi to Legendre*, Boston, etc. : Birkhäuser, 1983.
Western (Alfred Edward)
[1932] On Lucas' and Pépin's tests for the primeness of Mersenne's numbers, *Journal of the London Mathematical Society*, 7 (1932), p. 130–137.