COMPTES RENDUS

DES SÉANCES.

DE L'ACADÉMIE DES SCIENCES

SÉANCE DU LUNDI 5 JUIN 1876.

PRÉSIDENCE DE M. LE VICE-AMIRAL PÂRIS.

MÉMOIRES ET COMMUNICATIONS

DES MEMBRES ET DES CORRESPONDANTS DE L'ACADÉMIE.

ANALYSE MATHÉMATIQUE. — *Sur les rapports qui existent entre la théorie des nombres et le Calcul intégral* ; par M. **E. LUCAS**.

(Renvoi à l'examen de M. Puiseux.)

« Le but que nous nous proposons dans cette Note est de montrer l'identité des formules concernant certaines fonctions numériques des racines d'une équation du second degré à coefficients commensurables avec celles qui relient entre elles les fonctions circulaires, et d'indiquer, plus généralement, l'identité des formules concernant les fonctions numériques des racines d'une équation algébrique du quatrième degré ou de degré quelconque avec celles qui relient les transcendantes elliptiques ou abéliennes.

« Soient a et b les deux racines de l'équation du second degré, à coefficients entiers et premiers entre eux et, de plus,

$$a+b=\mathrm{P},\quad ab=\mathrm{Q},\quad a-b=\delta,\quad u_n=\frac{a^n-b^n}{a-b},\quad v_n=a^n+b^n,$$

les fonctions définies par les relations

$$\mathrm{S}(z)=\frac{\delta\sqrt{-1}}{2\mathrm{Q}^{\frac{n}{2}}}u_n,\quad \mathrm{C}(z)=\frac{1}{2\mathrm{Q}^{\frac{n}{2}}}v_n,\quad z=n\log\frac{a}{b}$$

sont entièrement analogues au sinus et au cosinus, et les formules qui les renferment, déduites de celles de la Trigonométrie, conduisent à des propriétés importantes des diviseurs de u_n et de v_n, lorsque n désigne un nombre entier.

« Les formules de l'addition et de la multiplication des arcs conduisent ainsi aux formules

(1) $u_{2n} = u_n v_n$, (2) $v_n^2 - \delta^2 u_n^2 = 4\mathrm{Q}^n$,

(3) $2u_{m+n} = u_m v_n + u_n v_m$ (4) $u_n^2 - u_{n-1}u_{n+1} = \mathrm{Q}^{n-1}$.

« Si l'on ne tient pas compte des diviseurs de Q et de δ^2, on en déduit les propositions suivantes :

« 1° Le terme u_{pq} est divisible par u_p et u_q, et par le produit $u_p u_q$, si p et q désignent des nombres premiers entre eux.

« 2° Les nombres u_n et v_n sont premiers entre eux.

« 3° Le plus grand commun diviseur de u_m et u_n est égal à u_d, en désignant par d le plus grand commun diviseur de m et de n.

« 4° En désignant par n un nombre impair, u_n est un diviseur de la forme quadratique $x^2 - \mathrm{Q}y^2$.

« Les développements de u_{np} et de v_{np} suivant les puissances de u_n et de v_n pris séparément on simultanément, sont entièrement analogues aux formules qui donnent sinnx et cosnx en fonction des puissances de sin$u$ et de cos$x$, et donnent lieu à un grand nombre de théorèmes concernant les formes quadratiques des diviseurs de u_{np} et de v_{np}

« On en déduit la loi de l'apparition des nombres premiers dans la série récurrente des u_n ; cette loi a été donnée par Fermat, lorsque δ est rationnel, et par Lagrange, lorsque δ est irrationnel. L'application de cette loi m'a permis de trouver un critérium général, indiquant et une équation numérique donnée, de degré quelconque, à coefficients commensurables, est ou n'est pas irréductible.

« Les développements de u_n^p et de v_n^p, en fonction linéaire des termes u et v, dont les rangs sont multiples de n, sont entièrement analogues aux formules de Moivre et de Bernoulli, qui donnent $\sin^p x$ et $\cos^p x$ en fonction des sinus et cosinus des multiples de l'arc x, et conduisent à *la loi de la répétition* des nombres premiers dans les séries des u_n et des v_n. Par exemple, lorsque n désigne le rang du premier terme contenant le facteur premier p à la puissance de λ, le terme u_{pn} sera le premier terme divisible par $p^{\lambda+1}$, et non par une puissance supérieure. Cette loi contient les propositions de MM. Arndt (*Journal de Crelle*, t. 31, p. 260, année 1846) et Sancery (*Bulletin de la Société mathématique*, t. IV, p. 17, année 1876).

« On a encore les propositions suivantes :

« 1° Si p désigne un nombre premier de la forme $4q + 1$ on de la forme $4q + 3$, les diviseurs du quotient de u_{pn} par u_n sont des diviseurs de la forme quadratique $x^2 - py^2$ ou de la forme $\delta x^2 + py^2$;

« 2° 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.

« La considération des diviseurs de u_n, lorsque n désigne les multiples on les puissances d'un nombre premier, ou encore un nombre quelconque, fait voir qu'il y a une infinité de nombres premiers communs aux deux formes $x^2 + \mathrm{Q}y^2$ et $x^2 - py^2$, si $p = 4q + 1$; et aux deux formes $x^2 + \mathrm{Q}y^2$ et $x^2 + py^2$ si

$p = 4q + 3$: elle donne des démonstrations simples de la loi de réciprocité et du théorème de Dirichlet, et conduit à certaines formules *ne contenant que des nombres premiers*.

« Dans un Mémoire présenté à l'Académie des Sciences de Turin (avril 1876), M. Genocchi, qui a bien voulu citer quelques-uns des résultats auxquels j'étais parvenu précédemment, rectifie une assertion de Legendre, que j'avais reproduite, sur le nombre premier $2^{31} - 1$. Il indique encore, suivant une assertion du P. Mersenne, un nombre probablement premier, et contenant 78 chiffre. A ce propos, je ferai observer que 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+1}, a étant égal à 2, 3 on 5.

« La construction de ce mécanisme permet de calculer rapidement, dans le système binaire de la numération, les résidus des v_n 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 de la géométrie du tissage. »