COMPTES RENDUS

DES SÉANCES.

DE L'ACADÉMIE DES SCIENCES

SÉANCE DU LUNDI 23 AOUT 1875.

PRÉSIDENCE DE M. FREMY.

MÉMOIRES ET COMMUNICATIONS

DES MEMBRES ET DES CORRESPONDANTS DE L'ACADÉMIE.

GÉOMÉTRIE. —*De la trisection de l'angle à l'aide du compas* ;

PAR M. **ÉD. LUCAS**.

« Dans une Lettre de Descartes au P. Mersenne, en date du 8 octobre 1629, on trouve le passage suivant :

« De diviser les cercles en 27 et 29, cela se peut mécaniquement, mais non point géométriquement ; il est vrai qu'il se peut en 27, par le moyen d'un cylindre, encore que peu de gens en puissent trouver le moyen, mais non pas en 29, et, si l'on *m'en* veut envoyer la démonstration, j'ose vous promettre de faire voir que cela n'est pas exact. » (*Oeuvres de Descartes*, par Cousin, t. VI, p. 56.)

« La construction des polygones réguliers de 9, 27, 81, … côtés se déduit du principe suivant, qui résout le problème de la trisection de l'angle en se servant de figures décrites à l'aide d'un compas sur la surface d'un cylindre de révolution. Soient, en effet, ABC la base d'un cylindre de rayon égal à l'unité, A l'origine des arcs, B et C les extrémités de l'arc donné *a* et de l'arc supplémentaire. Du point B comme centre on décrit sur la surface du cylindre une courbe sphérique passant par le point diamétralement opposé au point B; sur la génératrice passant par le point C, on prend un point D dont l'ordonnée est égale au cosinus de l'arc donné, et de ce point D comme centre on décrit sur la surface du cylindre une seconde courbe sphérique passant par le point diamétralement opposé au point C.

« Ces deux courbes se coupent en quatre points situés dans un plan, sur un même cercle, et dont les ordonnées sont égales à 2cos *a* et aux trois valeurs

de l'expression $2\cos\frac{a+2k\pi}{3}$. Les projections sur la circonférence de base de ces quatre points d'intersection sont les extrémités de quatre arcs respectivement égaux à 2π – a et aux trois valeurs cherchées de l'expression $\frac{a+2k\pi}{3}$.

« Telle est, je pense, l'interprétation que l'on doit donner du-passage de Descartes rapporté plus haut. La méthode employée permet aussi de construire les racines des équations du troisième et du quatrième degré. »

COMPTES RENDUS

DES SÉANCES.

DE L'ACADÉMIE DES SCIENCES

SÉANCE DU LUNDI 10 JANVIER 1876.

PRÉSIDENCE DE M. LE VICE-AMIRAL PÂRIS.

MÉMOIRES ET COMMUNICATIONS

DES MEMBRES ET DES CORRESPONDANTS DE L'ACADÉMIE.

ANALYSE. — *Note sur l'application des séries récurrentes à la recherche de la loi de distribution des nombres premiers ;* par M. **E. LUCAS**. (Extrait.)

« La série de Lamé, que cet illustre géomètre fit servir à la détermination d'une limite supérieure du nombre des opérations à effectuer dans la recherche du plus grand commun diviseur de deux nombres entiers, est une série récurrente définie par la relation

$$u_{n+2} = u_{n+1} + u_n,$$

et par les deux conditions initiales

$$u_0 = 0, \qquad u_1 = 1;$$

elle possède les propriétés suivantes :

« THEOREME I. — *L'expression d'un terme quelconque u_n est donnée, en fonction du rang n, par la formule*

$$2^n \sqrt{5} u_n = \left(1+\sqrt{5}\right)^n - \left(1-\sqrt{5}\right)^n.$$

« THEOREME II. — *On a les deux formules symboliques*

$$u^{n+2p} = u^n (u+1)^p,$$

$$u^{n-p} = u^n (u-1)^p,$$

dans lesquelles on remplace, après le développement, les exposants par des indices. Les trois formules précédentes subsistent encore lorsque l'on donne à n des valeurs négatives.

« THEOREME III. — *On a encore la formule*

$$u_{n+1} = 1 + \frac{n}{1} + \frac{(n-1)(n-2)}{1.2} + \frac{(n-2)(n-3)(n-4)}{1.2.3} + \dots ,$$

et l'expression

$$1 - \frac{n}{1} + \frac{(n-1)(n-2)}{1.2} - \frac{(n-2)(n-3)(n-4)}{1.2.3} + \dots ,$$

est égale à + 1, à 0 ou à – 1, *suivant que le reste de la division de n par* 6 *est* 0 *ou* 5, 1 *ou* 4, 2 *ou* 3.

« THEOREME IV. — *Le terme de rang pq est exactement divisible par les termes de rangs p et q, et par leur produit si les nombres p et q sont premiers entre eux.*

« On en déduit une proposition réciproque.

« THEOREME V. — *En posant* $u_{2n} = u_n v_n$, *la série des v représente des nombres entiers satisfaisant à la relation*

$$v_{n+2} = v_{n+1} + v_n,$$

et aux deux relations

$$v_{4n+2} = v_{2n+1}^2 + 2,$$
$$v_{4n} = v_{2n}^2 - 2.$$

Il est facile de trouver un grand nombre de formules analogues aux précédentes. Ces formules permettent de calculer rapidement les termes de la série de Lamé dont le rang est égal à $2^n k$, lorsque l'on connaît le terme de rang k.

« THEOREME VI. — *Les diviseurs premiers impairs de* u_{2n+1}, *sont de la forme* $4q + 1$ *; les diviseurs premiers impairs de* v_{4n} *sont de la forme* $8q \pm 1$, *et la diviseurs premiers impairs de* v_{4n+2} *sont des formes* $8q + 1$ *et* $8q + 3$.

« THEOREME VII. — *Si p désigne un nombre premier de la forme* $10q \pm 1$, *les termes dont le rang est un multiple quelconque d'un certain diviseur de* $p - 1$ *sont divisibles par p, et les autres termes ne sont pas divisibles par p.*

« THEOREME VIII. — *Si p désigne un nombre premier de la forme* $20q + 11$ ou *de la forme* $20q + 19$, les *termes divisibles par p ont pour rangs les nombres égaux aux multiples de* $p - 1$

« THEOREME IX. — *Si p désigne un nombre premier de la forme* $10q \pm 3$, *Les termes divisibles par p ont un rang égal à un multiple quelconque d'un certain diviseur de* $p + 1$.

« THEOREME X. — *Si le terme de rang* A + 1 *dans la série de Lamé est divisible par le nombre impair* A *de la forme* $10p \pm 3$, *et si aucun terme dont le rang est un diviseur de* A + 1 *n'est divisible par* A, *le nombre A est premier.*

« THEOREME XI. — *Si le terme de rang* A – 1 *dans la série de Lamé est divisible par le nombre impair* A *de la forme* $10p \pm 1$, *et si aucun terme dont rang est un diviseur de* A ± 1 *n'est divisible par* A, *le nombre A est le premier.*

« J'ai découvert un grand nombre d'autres propositions de ce genre, s'appliquant encore aux séries récurrentes contenant un terme nul, et en particulier à toutes les séries récurrentes déduites de la résolution des équations quadratiques, et en particulier de celle de Pell. Ces propositions permettent de décomposer rapidement les termes de la série de Lamé, par exemple, en leurs facteurs premiers, ou de reconnaître s'ils sont premiers. Ainsi

$$u_{2q} = 514229$$

n'admet que les diviseurs premiers des formes linéaires

$$116p + 1, \qquad 116p + 57,$$

et l'essai des deux nombres 173 et 349, qui satisfont à cette condition, indique immédiatement que u_{2q}, est un nombre premier.

« Il est d'ailleurs important de remarquer que les théorèmes X et XI permettent de savoir si un nombre est premier ou composé, sans qu'on ait besoin de se servir de la table des nombres premiers. C'est à l'aide de ces théorèmes que je pense avoir démontré que le nombre

$$A = 2^{127} - 1$$

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 $2^{31} - 1$.

« En effet, le nombre A est de la forme $10p - 3$, et j'ai vérifié que u_k n'est jamais divisible par A pour $k = 2^n$, excepté pour n égal à 127. »

M. L. Saltel adresse un Mémoire sur la théorie de l'élimination.

(Renvoi à la Commission précédemment nommée.)

M. Ed. Lucas adresse un Mémoire sur un nouveau système de Géométrie du cercle et de la sphère.

(Commissaires : MM. Puiseux, Bouquet.)

M. le vice-amiral Choppart transmet à l'Académie deux plis cachetés qui lui ont été adressés de Taïti. Ces plis portent l'épigraphe : « Je renais de mes cendres », et sont destinés au Concours pour la destruction du Phylloxera.

(Renvoi à la Commission du Phylloxera.)

MM. J. Deschamps, G. Le Falher, L. La Selve adressent des Communications relatives au Phylloxera.

(Renvoi à la Commission du Phylloxera.)

M. L. Paget adresse deux Notes, l'une sur une formule d'interpolation et l'autre sur une loi relative aux révolutions sidérales des planètes et à leurs distances au Soleil.

(Renvoi à la Section d'Astronomie.)

M. A. Brachet adresse une Note sur de nouveaux moyens d'étudier la fluorescence.

(Renvoi à la Commission précédemment nommée.)

CORRESPONDANCE.

M. Laussedat prie l'Académie de vouloir bien le comprendre parmi les candidats à la place d'Académicien libre, laissée vacante par le décès de M. *Séguier*.

(Renvoi à la future Commission.)

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) $v_n^2 - \delta^2 u_n^2 = 4Q^n$,

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

« 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 no mbre impair, u_n est un diviseur de la forme quadratique $x^2 - Qy^2$.

« 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 $x^2 + Qy^2$ et $x^2 - py^2$, si $p = 4q + 1$; et aux deux formes $x^2 + Qy^2$ 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. »

COMPTES RENDUS

DES SÉANCES.

DE L'ACADÉMIE DES SCIENCES

SÉANCE DU LUNDI 4 SEPTEMBRE 1876.

PRÉSIDENCE DE M. LE VICE-AMIRAL PÂRIS.

MÉMOIRES ET COMMUNICATIONS

DES MEMBRES ET DES CORRESPONDANTS DE L'ACADÉMIE.

ANALYSE. — *Théorie nouvelle des nombres de Bernoulli* et *d'Euler ;*
par M. **E. LUCAS**.

« **1.** Si l'on fait

$$f(x+1) - f(x) = A_0 x^n + A_1 x^{n-1} + \ldots + A_n ,$$

$$S_n = 1^n + 2^n + 3^n + \ldots + (x-1)^n ,$$

on obtient, en remplaçant successivement x par 1, 2, 3, ... $(x-1)$ dans la première équation, et en ajoutant la formule symbolique

$$f(x) - f(1) = f(S+1) - f(S), \tag{1}$$

dans laquelle on remplacera, après le développement du second membre, les exposants de S par des indices, et S, par $x-1$.

« **2.** On peut poser, symboliquement, la formule

$$nS_{n-1} = (x+B)^n - B^n , \tag{2}$$

dans laquelle on remplacera, après le développement du second membre, les exposants de B par des indices, et B_0 par 1. Les coefficients B représentent, avec une légère modification de l'indice, les nombres de Bernoulli. On voit d'ailleurs immédiatement, au moyen de la formule (1), qu'ils ne varient pas lorsque l'on augmente l'indice de S d'une unité.

« **3.** Si, dans la formule (2), on remplace x par $x+1$, on obtient l'identité

$$nx^{n-1} = (x+B+1)^n - (x+B)^n , \tag{3}$$

et, par suite, plus généralement, l'identité

$$f'(x) = f(x + B + 1) - f(x + B), \tag{4}$$

dans laquelle *f* désigne une fonction quelconque. En faisant successivement *x* *égal à* 0, ±1, ±2, ±½, dans la formule (3), on retrouve sans exception, toutes les relations connues servant au calcul des nombres de Bernoulli. En remplaçant dans l'équation (4)la fonction *f* par chacune des fonctions dont la différence est simple, comme la factorielle, l'exponentielle, le sinus, etc., on trouve toutes les formules dont le développement contient les nombres de Bernoulli, et beaucoup d'autres formules nouvelles.

4. En désignant par Δx la différence d'une fonction pour l'accroissement de *x* égal à l'unité, la relation (4) peut s'écrire, par l'introduction d'une autre variables sous la forme

$$\frac{\mathrm{d}f(x,y)}{\mathrm{d}x} = \Delta_x f(x+B,y),$$

et, en appliquant -cette formule à la fonction $\Delta x f(x,y)$, on a de même

$$\frac{\mathrm{d}^2(x,y)}{\mathrm{d}x\mathrm{d}y} = \Delta^2_{x,y} f(x+B,y+B'),$$

et encore

$$\frac{\mathrm{d}^3 f(x,y,z)}{\mathrm{d}x\mathrm{d}y\mathrm{d}z} \Delta^3_{x,y,z} f(x+B,y+B',z+B''). \tag{5}$$

« Dans le développement symbolique du second membre, on ne doit pas réduire les B avec les B' et avec les B'' ; mais ces formules donnent des relations entre les produits deux à deux, trois à trois, etc., des nombres de Bernoulli. La formule de M. Le Paige, donnée dans les *Bulletins de l'Académie de Belgique*, mai 1876, s'obtient en supposant simplement

$$f(x,y) = x^m y^m .$$

5. La formule (1), peut aussi être généralisée, et l'on a ainsi, pour la fonction $f(x, y, z)$, la formule

$$\Delta^3_{x=x,y=y,z=z} f(0,0,0) = \Delta^3_{s=1,s'=1,s''=1} f(\mathrm{S},\mathrm{S}',\mathrm{S}'') \tag{6}$$

« On peut aussi exprimer les produits $\mathrm{B}_m\mathrm{B}_n\mathrm{B}_p$ et $\mathrm{S}_m\mathrm{S}_n\mathrm{S}_p$ en fonction linéaire des B et des S ; en retrouvera ainsi comme cas particulier la formule

$$2\mathrm{S}_3^2 = \mathrm{S}_7 + \mathrm{S}_5$$

indiquée par Jacobi (*Lettre de Schumacher à Gauss*, en date du 12 avril 1847), et l'on pourra en trouver une série indéfinie d'autres semblables.

« **6.** Les nombres analogues à ceux de Bernoulli, considérés par Euler, et par MM. Sylvester et Catalan (*Comptes rendus*, t. LII, p. 161; t. LIV, p. 1033) donnent lieu aux mêmes développements. Si l'on pose

$$\mathrm{P}_n = 2(2^n - 1)\mathrm{B}_n$$

et

$$\sigma_n = 1^n - 2^n + 3^n - 4^n + \ldots + (2x-1)^n ,$$

on déduit, en changeant x en $\frac{x}{2}$ dans la formule (2), et en retranchant,

$$2n\sigma_{n-1} = P^n - (2x + P)^n,$$

en ayant soin de remplacer P_0 par 0. Les fonctions σ_n jouissent de propriétés curieuses, analogues à celles des fonctions S_n (BERTRAND, *Calcul différentiel*, t. I, p. 352). On trouve aisément, pour les P et les σ, des formules semblables aux formules (5) et (6), et, par suite, une démonstration immédiate de cette propriété connue, que les nombres P sont entiers. On a encore, pour le nombre premier p, la congruence

$$nP_{n+p-1} \equiv (n-1)P_n \pmod{p},$$

et un grand nombre d'autres qui permettent d'appliquer le calcul de ces nombres à la recherche des grands nombres premiers. »

COMPTES RENDUS

DES SÉANCES.

DE L'ACADÉMIE DES SCIENCES

SÉANCE DU LUNDI 27 DECEMBRE 1876.

PRÉSIDENCE DE M. LE VICE-AMIRAL PÂRIS.

MÉMOIRES ET COMMUNICATIONS

DES MEMBRES ET DES CORRESPONDANTS DE L'ACADÉMIE.

ANALYSE, — *Nouveaux théorèmes d'Arithmétique supérieure.*
Note de M. **ÉD. LUCAS**.

« J'ai indiqué, dans diverses Communications précédentes[1] un nouveau procédé propre à la recherche des grands nombres premiers ou à la décomposition des grands nombres en leurs facteurs. La comparaison des séries récurrentes de Fibonacci et de Fermat, ou, plus généralement *des fonctions numériques simplement périodiques*, donne lieu à beaucoup de théorèmes curieux parmi lesquels nous citerons seulement les suivants

« *I. — Soit le nombre*

$$p = 2^{4m+3} - 1 ,$$

dont l'exposant est supposé premier. On forme la série

$$3,\ 7,\ 47,\ 2207,\ \ldots \qquad \text{avec} \qquad r_{n+1} = r_n^2 - 2 .$$

Le nombre p est premier lorsque le rang du premier terme divisible par p occupe le rang $4m + 2$; *le nombre p est composé si aucun des* $4m + 2$ *premiers termes de la série n'est divisible par p* ; *enfin, si* α *désigne le rang du premier terme divisible par p, les diviseurs de p sont de la forme linéaire* $2^{\alpha}k \pm 1$ *combinée avec celles des diviseurs de* $x^2 - 2y^2$.

1 *Comptes Rendus*, 10 janvier et 5 juin 1876. — *Atti della reale Acedemia delle Scienze di Torino*, mai 1876.

« On prendra seulement les résidus par rapport au module p ; ainsi, pour le nombre $2^{31} - 1$ que j'ai pris naguère pour exemple, r_{30} aurait, sans cette simplification, plus de *deux-cent millions* de chiffres, dans le système décimal. Le mécanisme dont j'ai parlé s'appliquera à tous les nombres de cette forme, et, avec quelques modifications, à ceux des formes suivantes, dont les calculs présentent, dans le système de numération binaire ou ternaire, des avantages considérables.

« *II* — Soit le nombre

$$p = 3.2^{4m+2} + 1 .$$

On forme les $4m + 3$ *premiers termes de la série*

$$2,\ 9,\ 161,\ 51841, \ldots \quad \text{avec} \quad r_{n+1} = 2\,r_n^2 - 1 .$$

Le nombre p est premier lorsque le rang du premier terme divisible par p est égal à $4m + 3$; *le nombre p est composé si aucun des termes de la série n'est divisible par p. Si* α *désigne le rang du premier terme divisible par p, les diviseurs de p sont de la* forme $3.2^{\alpha}k \pm 1$, *combinée avec celles des, diviseurs de* $x^2 - 2y^2$ *et de* $x^2 - 6y^2$.

« *III.*— Soit le nombre

$$p = 2.3^{4m+2} + 1.$$

On forme les $4\,m + 2$ *premiers termes de la série*

$$4,\ 19,\ 57\ 79, \ldots \quad \text{avec} \quad r_{n+1} = r_n^3 - 3r_n^2 + 3 .$$

Le nombre p est premier lorsque le rang du premier terme divisible par p occupe le rang $4m + 2$ *; il est composé si aucun des* $4m + 2$ *premiers résidus n'est égal à zéro. Enfin, si a désigne le rang du premier résidu nul, les diviseurs de p sont de la forme linéaire* $2.3^{\alpha}k \pm 1$, *combinée avec celles des diviseurs des formes quadratiques* $x^2 + 2y^2$ *et* $x^2 + 3y^2$.

« IV. — Soit le nombre

$$p = 2.3^{4m+2} - 1 \quad \text{ou} \quad p = 2.^{34m+3} - 1 .$$

On forme la série

$$2,\ 17,\ 5777, \ldots \quad \text{avec} \quad r_{n+1} = r_n^3 - 3r_n^2 - 3 .$$

Le nombre p est premier lorsque le rang du premier résidu nul est égal à $4m +$ (2 ou 3) ; *il est composé si aucun des* $4m +$ (2 ou 3) *premiers termes n'est divisible par p. De plus, si* α *désigne le rang du premier résidu nul, les diviseurs de p ont la forme linéaire* $2.3^{\alpha}k \pm 1$, *combinée avec celles des diviseurs de* $5x^2 - 3y^2$ et *de* $x^2 - 2y^2$ dans *le premier cas, et* de $x^2 - 6y^2$ *dans le second.*

« On observera que la différence des termes correspondants dans les deux séries précédentes est égale à 2.

« Exemple. — Pour $p = 2.3^{\chi} - 1$, les résidus sont 2, 17, l404, 0 ; donc p est premier, puisqu'il n'a pas de diviseur intérieur à sa racine carrée.

« *V. — Soit, le nombre*

$$p = 2.5^{2m+1} + 1$$

On forme la série limitée à $2m + 1$ *termes*

$$11,\ 167761, \ldots \quad \text{avec} \quad r_{n+1} = r_n^5 + 5r_n^2 + 5r_n .$$

Le nombre p est premier lorsque le rang du premier résidu nul est égal à $2m + 1$; *il est composé si aucun des termes n'est divisible par p. Enfin, si a désigne le rang du premier résidu égal à zéro, les diviseurs premiers de p sont de la forme* $2.5^{\alpha}k + 1$

« On obtient des théorèmes analogues en remplaçant les nombres 2, 3 et 5 par des nombres premiers quelconques, en changeant la loi de formation de la série. On peut d'ailleurs augmenter les coefficients des puissances de 2, 3, 5 ou d'un nombre premier quelconque, d'un multiple de 10, sans changer les résultats précédents mais il faut alors remplacer les deux premiers termes des séries récurrentes considérées précédemment. »

dans la couche superficielle du vitellus, plusieurs enfin immergés dans le liquide accumulé entre le vitellus et la vitelline. Parmi ces derniers, j'en vis deux encore très-mobiles, nageant çà et là, changeant de direction, tantôt s'efforçant de pénétrer dans le vitellus, tantôt s'en détournant, et cela plus de dix heures après le début de l'imprégnation spermique de l'œuf, qui n'avait été entravée ni par la mort de la lapine, ni par l'isolement et le refroidissement de l'appareil génital. A l'exception de ces deux spermatozoïdes, tous les autres, y compris ceux qui furent obtenus par le raclage des parties libres de la muqueuse, étaient immobiles. Je voulus ensuite continuer l'examen avec un objectif 10 à long foyer, me servant, pour liquide d'immersion, d'une gouttelette de sérosité péritonéale. Mais, dans ces nouvelles conditions, je vis l'œuf se mettre en mouvement, d'une manière lente et régulière, et sortir du champ. Je retrouvai l'œuf immobile un peu plus loin, en me servant d'un objectif 4 à sec. Je renouvelai alors l'expérience avec le 10 à immersion, et l'œuf fut mis de nouveau en mouvement et disparut.

» Cette observation me paraît jeter une assez grande lumière sur ce que j'appelle les conditions de la vie et de la survie des spermatozoïdes au sein de l'œuf des Mammifères. Elle suggère aussi d'intéressantes conclusions sur les phénomènes intimes de la fécondation; j'espère que je pourrai les formuler plus tard, lorsque les recherches que j'ai commencées à ce sujet dans le laboratoire de Physiologie du Muséum seront plus avancées. »

M. **J. de Cossigny** adresse des Observations relatives à la Note communiquée par M. *A. Leplay*, dans la séance du 18 décembre 1876, sur l'absorption des principes fertilisants par une prairie.

M. **Ed. Lucas** adresse quelques observations critiques, au sujet des énoncés de théorèmes sur les nombres qui ont été communiqués par M. *F. Proth*, dans la séance du 27 décembre 1876.

M. **A.-L. Donnadieu** adresse une Note relative à une masse qui a été trouvée dans la cavité abdominale d'un canard, et qui est formée par un faisceau de plumes ayant subi un arrêt de développement.

M. **H. Comte** adresse une Note concernant la « machine parlante » de *Faber*.

M. **J. Laugé** adresse la description d'un tourbillon dont il a été témoin, et dans lequel la direction de l'air a pu être déterminée par celle de la paille enlevée à une prairie.

COMPTES RENDUS

DES SÉANCES.

DE L'ACADÉMIE DES SCIENCES

SÉANCE DU LUNDI 5 MARS 1877.

PRÉSIDENCE DE M. PELIGOT.

MÉMOIRES ET COMMUNICATIONS

DES MEMBRES ET DES CORRESPONDANTS DE L'ACADÉMIE.

ANALYSE MATHÉMATIQUE. — *Sur l'extension du théorème de Fermat généralisé, et du* Canon arithmeticus ; par M. **ÉD. LUCAS.**

« Nous avons indiqué (*Comptes rendus,* 10 janvier, 5 juin et 27 décembre 1876), l'application des *fonctions numériques simplement périodiques*

$$U_n = \frac{a^n - b^n}{a - b} \quad \text{et} \quad V_n = a^n + b^n$$

des racines a et b d'une, équation quadratique à coefficients commensurables et premiers entre eux

$$x^2 = Px - Q$$

à l'étude des propriétés générales des nombres.

« Soit p un nombre premier, non diviseur de Q, et $\Delta = (a - b)^2$; on sait[1] que les termes U_n divisibles par p ont un rang égal à tous les multiples d'un certain diviseur θ de $p + \left(\frac{\Delta}{p}\right)$, en désignant par la notation $\left(\frac{\Delta}{p}\right)$ le reste de $\Delta^{\frac{p-1}{2}}$ par p ; ce reste est égal à 0, +1, ou –1, suivant que Δ est un multiple, un résidu quadratique, où un non-résidu quadratique de p ; de plus, la *loi de répétition* des nombres premiers, dans ces séries récurrentes, indique 1e terme U_n de rang $n = p^{\lambda}\theta$ est divisible par $p^{\lambda+1}$.

1 *Atti della R. Accademia delle Scienze di Torino,* mai 1876.

« Soit maintenant m un nombre quelconque décomposé en ses facteurs premiers, que l'on ne suppose pas diviseurs de Q,

$$m = p^{\varpi} r^{\rho} s^{\sigma} \ldots$$

et

$$\psi(m) = p^{\varpi-1} r^{\rho-1} s^{\sigma-1} \ldots \left[p - \left(\frac{\Delta}{p}\right)\right]\left[r - \left(\frac{\Delta}{r}\right)\right]\left[s - \left(\frac{\Delta}{s}\right)\right] \ldots ;$$

on a le *théorème fondamental donné* par la congruence

$$U_{\Psi(m)} \equiv 0 \pmod{m} ;$$

de plus, les termes U_n divisibles par m sont ceux, dont le rang n est un multiple quelconque d'un certain diviseur μ de $\Psi(m)$. Ce nombre μ est, par extension, l'exposant auquel appartient a ou b par rapport au module m ; d'ailleurs, on retrouve le théorème de Fermat généralisé par Euler, en supposant $b = 1$. L'application du théorème fondamental conduit à la connaissance du procédé que nous avons indiqué pour la vérification des nombres premiers. Ce procédé repose sur le théorème suivant, qui est, en quelque sorte, l'inverse du précédent. Si $U_{p\pm1}$ *est divisible par p sans qu'aucun des diviseurs de p* ± 1 *le soit, le nombre p est premier.*

« Soient, pour plus de simplicité (bien que la méthode s'applique à tous les nombres p, tels que la décomposition de $p \pm 1$ en facteurs premiers soit connue), P = 1, Q = – 1 et $p = 2^{4q+3} - 1$, Q = – 1, l'exposant $4^q + 3$ étant premier. On a évidemment

$$U_{2n} = U_n V_n, \qquad V_{2n} = V_n^2 - 2(-1)^n ;$$

on forme les nombres

$$V2,\ V4,\ V6, \ldots V_{p+1} \quad \text{ou} \quad 1,\ 3,\ 7,\ 47,\ 2207, \ldots ,$$

tels que chacun d'eux- est égal au carré du précédent diminué de deux unités, et l'on prend, les résidus par rapport au module p. Si le premier des termes divisibles par p est égal à $4q + 2$, le nombres est premier. On peut encore énoncer ce résultat sous cette forme :

« THEOREME. — *Pour que le nombre* $p = 2^{4q+3} - 1$ *soit premier, il faut que la congruence*

$$3 \equiv 2\cos\frac{\pi}{2^{2q+1}} \pmod{2^{4q+3} - 1}$$

soit satisfaite après la disparition des radiaux, et il suffit que le premier membre de cette congruence ne s'annule *pas dans la première moitié de l'opération.*

« Soit, par exemple, $p = 2^{19} - 1$; on simplifie le calcul par l'emploi du système de numération binaire qui supprime les multiplications et les divisions ; le résidu de $V_{2^{13}}$ s'écrit, dans ce système,

$$110010111000101001 ;$$

si l'on observe que les restes de 2^{19}, 2^{20}, 2^{21}, . . . par p sont respectivement 1, 2, 2^2, . . . , le carré de $V_{2^{13}}$ se dispose, en supprimant les multiples de $2^{19} - 1$, de la manière suivante :

18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
0	1	1	0	0	1	0	1	1	1	0	0	0	1	0	1	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	1	1	1	0	0	0	1	0	1	0	0	1	0	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	0	0	0	1	0	1	0	0	1	0	1	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	0	1	0	0	1	0	1	1	0	0	1	0	1	1
0	0	0	1	0	1	0	0	1	0	1	1	0	0	1	0	1	1	1
0	0	1	0	1	0	0	1	0	1	1	0	0	1	0	1	1	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	0	0	1	0	1	1	0	0	1	0	1	1	1	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	1	1	0	0	1	0	1	1	1	0	0	0	1	0	1
0	1	0	1	1	0	0	1	0	1	1	1	0	0	0	1	0	1	0

« On fait une première addition, en ayant soin de retrancher une unité de la colonne 1, comme il suit :

1	0	0	1	0	1	0	0	1	0	0	1	1	0	0	1	0	0	1	A
1	1	1	1	0	1	0	0	0	1	0	1	0	1	1	0	0	0	1	B
1	0	1	1	0	1	1	1	1	1	0	1	0	1	1	1	1	0	0	C

« La ligne A contient les unités provenant de l'addition de chacune des colonnes ; la ligne B contient les unités du second ordre de l'addition de la colonne à droite ; la ligne C contient les unités du troisième ordre provenant de l'addition de la seconde colonne à. droite. Une addition donne enfin, pour le résidu de $V_{2^{14}}$:

0	1	0	0	0	0	0	0	1	1	0	0	0	1	1	1	0	0	0	

« En répétant 19 fois cette opération, on forme le tableau des résidus des V_{2^λ} suivant le module $2^{19} - 1$. Le dernier de ces résidus est nul ; donc $2^{19} - 1$ est premier.

« Tel est le principe fondamental sur lequel repose la *machine arithmétique propre à vérifier les grands nombres premiers ou à la décomposition des grands nombres en leurs facteurs.* »

COMPTES RENDUS

DES SÉANCES.

DE L'ACADÉMIE DES SCIENCES

SÉANCE DU LUNDI 16 JUILLET 1877.

PRÉSIDENCE DE M. PELIGOT.

MÉMOIRES ET COMMUNICATIONS

DES MEMBRES ET DES CORRESPONDANTS DE L'ACADÉMIE.

GÉOMÉTRIE. — *Sur la division de la circonférence en parties égales ;* Note de M. **ÉD. LUCAS**, présentée par M. Chasles.

« La théorie de la division géométrique de la circonférence en parties égales est traitée dans la dernière Section des *Disquisitiones arithmeticæ*. *Il* est convenu que cette opération ne peut être exécutée que des trois manières suivantes : 1° par l'emploi simultané de la règle et du compas, comme dans la construction ordinaire du décagone régulier (EUCLIDE) ; 2° par l'emploi du compas sans la règle (MASCHERONI) ; 3° par l'emploi de la double règle, sans compas, c'est-à-dire d'une règle plate dont les deux bords sont rectilignes et parallèles. Cette idée ingénieuse est due à M. de Coatpont, colonel du génie.

« Gauss a démontré que, pour diviser la circonférence en N parties égales, il faut et il suffit que

$$N = 2^{\mu} \times a_i \times a_j \times a_k \times \ldots,$$

μ étant arbitraire, et a_i, a_j, a_k, . . . des nombres premiers et différents, en nombre quelconque, mais de la forme

$$a_n = 2^{2^n} + 1$$

On a, pour les premières valeurs de n, les nombres premiers

$$a_0 = 3, \quad a_1 = 5, \quad a_2 = 17, \quad a_3 = 257, \quad a_4 = 65537.$$

Euler a démontré, contrairement à une assertion de Fermat, que a_5 n'est pas premier, puisque

$$a_5 = 2^{2^5} + 1 = 641 \times 6700417 ;$$

ainsi a, ne peut être compris dans l'expression de N ; mais il reste deux questions importantes à résoudre :

« 1° Comment peut-on continuer le tableau des nombres premiers a_n ? »

« 2° Existe-t-il une série indéfinie de nombres premiers de cette forme ?

« L'objet de cette Note est la réponse à la première question ; mais d'abord nous ferons observer que, pour savoir si le nombre

$$a_6 = 2^{2^6} + 1 = 18446744073709551617$$

est premier ou composé, l'application de toutes les méthodes connues jusqu'à présent (même en tenant compte de la forme linéaire $128q + 1$ des diviseurs de a_6) nécessiterait *trois mille ans* de travail assidu. Par le procédé suivant, il suffit de former successivement les carrés de soixante nombres ayant vingt chiffre au plus ; ce calcul peut être effectué en *trente heures*. Soit, en effet,

$$\sqrt{2}\,U_\lambda = \left(1+\sqrt{2}\right)^\lambda - \left(1-\sqrt{2}\right)^\lambda ;$$

on forme la série des nombres

$$U_1 = 2, \quad U_2 = 2^2.3, \quad U_3 = 2^3.3.17, \quad U_4 = 2^4.3.17.577,$$

$$U_5 = 2^5.3.17.577.665857, \ldots ;$$

chacun des nouveaux facteurs est premier avec tous les précédents, et égal au double du carré du précédent diminué de l'unité ; cela posé, on a le théorème suivant, qui n'est qu'un cas particulier d'un théorème énoncé précédemment *(Comptes rendus,* 5 juin 1876).

« THEOREME. — *Soit le nombre* $a_n = 2^{2^n} + 1$; *on forme la série des* $2^n - 1$ *nombres*

$$3, \quad 17, \quad 577, \quad 665857, \quad 886731088997, \ldots ,$$

tels que chacun deux 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 ; *enfin, si* α *désigne le rang du premier terme divisible par* a_n, *les diviseurs premiers de* a_n *appartiennent à la forme linéaire*

$$2^{2^{n+1}} q + 1$$

Il est indispensable de calculer les résidus des nombres U_1, U_2, U_4, U_8, …, suivant le module a_n, au moyen de simples soustractions des dix premiers multiples de a_n ; ainsi, pour $n = 6$, la caractéristique du logarithme ordinaire de U_{a_6} est supérieure à 5×10^{18} ; il faudrait donc, rien que pour écrire le nombre U_{a_6} à raison de dix chiffres par seconde, un temps supérieur à *deux cents millions de siècles*. Je fais exécuter en ce moment les calculs concernant les nombres a_6 et a_7.

« 2. La considération des termes des séries récurrentes, dont les arguments sont en progression géométrique, conduit non-seulement à la recherche des grands nombres premiers, mais encore aux développements des irrationnelles du second degré et de leurs logarithmes en séries de fractions dont les dénominateurs sont composés de facteurs premiers entre eux deux à deux. Soient, en général,