THÉORIE DES FONCTIONS NUMERIQUES SIMPLEMENT PÉRIODIQUES

PAR EDOUARD LUCAS, *Professeur au Lycée Charlemagne, Paris.*

CE mémoire a pour objet l'étude des fonctions symétriques des racines d'une équation du second degré, et son application à la théorie des nombres premiers. Nous indiquons dès le commencement, l'analogie complète de ces fonctions symétriques avec les fonctions circulaires et hyperboliques ; nous montrons ensuite la liaison qui existe entre ces fonctions symétriques et les théories des déterminants, des combinaisons, des fractions continues, de la divisibilité, des diviseurs quadratiques, des radicaux continus, de la division de la circonférence, de l'analyse indéterininée du second degré, des résidus quadratiques, de la décomposition des grands nombres en facteurs premiers, etc. Cette méthode est le point de départ d'une étude plus compléte, des propriétés des fonctions symétriques des racines d'une équation algébrique, de degré quelconque, à coefficients commensurables, dans leurs rapports avec les théories des fonctions elliptiques et abéliennes, des résidus potentiels, et de l'analyse indéterminée des degrés supérieurs.

SECTION I.

Définition des fonctions numériques simplement périodiques.

Désignons par a et b les deux racines de l'équation

$$x^2 = Px - Q , \tag{1}$$

dont les coefficients P et Q sont des nombres entiers, positifs ou négatifs, et premiers entre eux. On a

$$a + b = P , \qquad ab = Q ;$$

et, en désignant par δ la différence $a - b$ des racines, et par Δ le carré de cette différence, on a encore

$$a = \frac{P+\delta}{2} , \qquad b = \frac{P-\delta}{2} , \qquad \delta = \sqrt{\Delta} = \sqrt{P^2 - 4Q} .$$

Cela posé, nous considérerons les deux fonctions numériques U et V définies par les égalités

$$(2) \qquad U_n = \frac{a^n - b^n}{a - b}, \qquad V_n = a^n + b^n$$

Ces fonctions U_n et V_n donnent naissance, pour toutes les valeurs entières et positives de n, à trois séries d'espèces différentes, selon la nature des racines a *et* b de l'équation (1). Cette équation peut avoir :

1°. Les racines réelles et entières ;

2°. Les racines réelles et incommensurables ;

3°. Les racines imaginaires.

Les *fonctions numériques de première espèce* correspondent à toutes les valeurs entières de a et de b, et peuvent être calculées directement, pour toutes les valeurs entières et positives de n, par l'emploi des formules (2). Si l'on suppose plus particulièrement $a = 2$ et $b = 1$, on trouve, en formant les valeurs de U_n et de V_n, les séries récurrentes

n :	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11, ...
U_n :	0,	1,	3,	7,	15,	31,	63,	127,	255,	511,	1023,	2047, ...
V_n :	2,	3,	5,	9,	17,	33,	65,	129,	257,	513,	1025,	2049, ...

étudiées pour la première fois par l'illustre FERMAT. Nous observerons, dès maintenant, que la série des V_n est contenue, pour les trois cas que nous considérons, dans la série des U_n, puisque les formules (2) nous donnent la relation générale

$$(3) \qquad U_{2n} = U_n V_n .$$

Les fonctions numériques de seconde espèce correspondent à toutes les valeurs incommensurables de a et de b dont la somme et le produit sont commensurables. On peut les calculer en fonction de la somme P et du discriminant Δ de l'équation proposée, au moyen des formules suivantes. Le développement du binôme nous donne

$$2^n a^n = P^n + \frac{n}{1} P^{n-1}\delta + \frac{n(n-1)}{1.2} P^{n-2}\delta^2 + \frac{n(n-1)(n-2)}{1.2.3} P^{n-3}\delta^3 + \ldots + \delta^n ,$$

$$2^n b^n = P^n - \frac{n}{1} P^{n-1}\delta + \frac{n(n-1)}{1.2} P^{n-2}\delta^2 - \frac{n(n-1)(n-2)}{1.2.3} P^{n-3}\delta^3 + \ldots + (-\delta)^n ;$$

et, par soustraction et par addition,

$$(4)\quad \begin{cases} 2^{n-1}U_n = \dfrac{n}{1}P^{n-1} + \dfrac{n(n-1)(n-2)}{1.2.3}P^{n-3}\Delta \\ \qquad\qquad + \dfrac{n(n-1)(n-2)(n-3)(n-4)}{1.2.3.4.5}P^{n-5}\Delta^2 + \ldots\ldots, \\ 2^{n-1}V_n = P^n + \dfrac{n(n-1)}{1.2}P^{n-2}\Delta + \dfrac{n(n-1)(n-2)(n-3)}{1.2.3.4}P^{n-4}\Delta^2 + \ldots\ldots \end{cases}$$

On obtient ainsi, pour les premiers termes,

$U_0 = 0, \quad U_1 = 1, \quad U_2 = P, \quad U^3 = P^2 - Q, \quad U_4 = P^3 - 2PQ,$

$V_0 = 2, \quad V_1 = P, \quad V_0 = P^2 - 2Q, \quad V_3 = P^3 - 3PQ \quad V_4 = P^4 - 4P^2Q + 2Q^2.$

Les fonctions numériques de seconde espèce les plus simples correspondent aux hypothèses

$$P = 1, \qquad Q = -1, \qquad \Delta = 5,$$

ou à l'équation

$$x^2 = x + 1 ;$$

on a dans ce cas,

$$a = 2\sin\frac{3\pi}{10} = \frac{1+\sqrt{5}}{2}, \qquad b = -2\sin\frac{\pi}{10} = \frac{1-\sqrt{5}}{2},$$

et, par suite, en désignant par u_n et v_n les fonction qui en résultent,

$$u_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}, \qquad v_n = \frac{(1+\sqrt{5})^n + (1-\sqrt{5})^n}{2^n}.$$

On forme ainsi, pour les premières valeurs de *n* entières et positives, les séries

n :	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11, ...
u_n :	0,	1,	l,	2,	3,	5,	8,	13,	21,	34,	55,	89, ...
v_n :	2,	1,	3,	4,	7,	11,	18,	29,	47,	76,	123,	199, ...

La série des u_n a été considérée pour la première fois par LEONARD FIBONACCI, de Pise.[*] Elle a été étudiée par ALBERT GIRARD,[†] qui a observé que les trois nombres u_n , u_n , u_{n+1} , forment un triangle isoscèle dont l'angle au sommet est à fort peu près égal à l'angle du pentagone régulier. ROBERT SIMPSON[‡] a fait

[*] *Il liber Abbaci di Leonardo Pisano, pubblicato secondo la lezione del Codice Magliabechiano, da* B. BONCOMPAGNI. Roma, 1867. Pag. 283 et 284.

[†] *L'arithmétique de* SIMON STEVIN, *be Bruges, revue, corrigée et augmentée de plusieurs traictez et annotations par* ALBERT GIRARD, etc. Leide, 1633. Pag. 169 et 170.

[‡] *Philosophical Transactions of the Royal Society of London,* Vol. xlviii, Part 1, for the year 1753.

remarquer en 1753, que cette série est donnée par le calcul des quotients et des fractions convergentes des expressions irrationnelles

$$\frac{\sqrt{5}+1}{2} \quad \text{et} \quad \frac{\sqrt{5}-1}{2} \ .$$

En 1843, J. BINET* donne, au moyen de cette série, l'expression du dénombrement des combinaisons discontinues. En 1844, Lamé† indique l'application que l'on peut faire de cette série à la détermination d'une limite supérieure du nombre des operations à faire dans la recherche du plus grand commun diviseur de deux nombres entiers.

Nous prendrons aussi quelquefois pour exemple la série U_n de seconde espèce, donnée par les hypothèses

$$P = 2, \qquad Q = -1, \qquad \Delta = 2^2.2,$$

ou par l'équation

$$x^2 = 2x + 1.$$

On a alors les séries

n :	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11, . . .
U_n :	0,	1,	2,	5,	12,	29,	70,	169,	408,	985,	2378,	5741, . . .
V_n :	2,	2,	6,	14,	34,	82,	198,	478,	1154,	2786,	6786,	*16238*, . . .

que nous désignerons sous le nom de SERIES DE PELL , en l'honneur du mathématicien de ce nom qui résolut, le premier, un célèbre problème d'analyse indéterminée proposé par FERMAT, et concernant la résolution en nombres entiers, de l'équation indéterminée

$$x^2 - \Delta y^2 = \pm 1.$$

Les *fonctions numériques de troisième espèce* correspondent à toutes les valeurs imaginaires de a et de b dont la somme et le produit sont réels et commensurables. Les plus simples proviennent des hypothèses

$$P = 1, \qquad Q = 1, \qquad \Delta = -3 \ ;$$

on a, dans ce cas,

$$a = \frac{1+\sqrt{-3}}{2}, \qquad b = \frac{1-\sqrt{-3}}{2}$$

par conséquent a et b sont les racines cubique imaginaires de l'unité négative ; de plus,

$$U_{3n} = 0, \qquad U_{3n+1} = (-1)^n, \qquad U_{3n+2} = (-1)^n.$$

An explication of an obcure passage in Albert Girard's Commentary upon Simon Stevin's Works. Pag. 368 et suiv.

* *Comptes rendus de l'académie des sciences de Paris*, tome, xvii, pag. 562 ; tome xix, pag. 939.

† *Comptes rendus*, etc., tome xix, pag. 867.

Ainsi les valeurs de U_n, reviennent périodiquement dans l'ordre

$$0, 1, 1, 0, -1, -1, \ldots\ldots$$

et donnent lieu à un grand nombre de formules simples déduites des propriétés générales des fonctions U_n, et V_n, et concernant la trisection de la circonférence.

Quelquefois aussi nous considérerons les séries analogues déduites de l'équation

$$x^2 = 2x - 2,$$

dans laquelle

$$a = 1 + \sqrt{-1}, \qquad b = 1 - \sqrt{-1}, \qquad \Delta = -2^2,$$

et les séries déduites de l'équation

$$x^2 = 2x - 3,$$

dans laquelle

$$a = 1 + \sqrt{-2}, \qquad b = 1 - \sqrt{-2}, \qquad \Delta = -2^2,$$

nous désignerons les séries obtenues dans cette dernière hypothèse, sous le nom de *séries conjuguées* de PELL.

SECTION II.

Des relations des fonctions U_n et V_n avec les fonctions circulaires et hyperboliques.

Si l'on fait $$z = \frac{n}{2} \text{ Log.nép.} \frac{a}{b},$$

dans les formules

$$\cos(z\sqrt{-1}) = \frac{e^z + e^{-z}}{2},$$

$$\sin(z\sqrt{-1}) = \frac{e^z - e^{-z}}{2\sqrt{-1}},$$

on obtient

$$\cos\left(\frac{n\sqrt{-1}}{2}\text{Log.}\frac{a}{b}\right) = \frac{1}{2}\left[\frac{a^{\frac{n}{2}}}{b^{\frac{n}{2}}} + \frac{b^{\frac{n}{2}}}{a^{\frac{n}{2}}}\right],$$

$$\sin\left(\frac{n\sqrt{-1}}{2}\text{Log.}\frac{a}{b}\right) = \frac{1}{2\sqrt{-1}}\left[\frac{a^{\frac{n}{2}}}{b^{\frac{n}{2}}} - \frac{b^{\frac{n}{2}}}{a^{\frac{n}{2}}}\right];$$

on a donc, entre, les fonctions U_n et V_n, et les fonctions circulaires, les deux relation

$$(5)\quad \begin{cases} V_n = 2Q^{\frac{n}{2}}\cos\left(\dfrac{n\sqrt{-1}}{2}\operatorname{Log}.\dfrac{a}{b}\right), \\ U_n = \dfrac{2Q^{\frac{n}{2}}}{\sqrt{-\Delta}}\sin\left(\dfrac{n\sqrt{-1}}{2}\operatorname{Log}.\dfrac{a}{b}\right) \end{cases}$$

Il résulte immédiatement de ce rapprochement que chacune des formules de la trigonométrie rectiligne couduit à des formules analogues pour U_n et V_n, et inversement.

Ainsi la formule (3)

$$U_{2n} = U_n V_n ,$$

correspond à la formule

$$\sin 2z = 2 \sin z \cos z ;$$

les équations

$$(6)\qquad V_n + \delta Un = 2a^n , \qquad V_n - \delta Un = 2b^n$$

que l'on déduit immédiatement des formules (2) correspondent exactement aux relations

$$\cos z + \sqrt{-1}\sin z = e^{z\sqrt{-1}}, \qquad \cos z - \sqrt{-1}\sin z = e^{-z\sqrt{-1}},$$

et les formules (4) sont entièrement analogues à celles qui ont été données dans *Actes de Leipzick,* en 1701, par JEAN BERNOULLI, pour le développement de $\dfrac{\sin nz}{\sin z}$ et de cos *nz* suivant les puissances du sinus et du cosinus de l'arc *z*.

Ainsi encore les formules

$$(7)\quad \begin{cases} [V_m + \delta U_m]\,[V_n + \delta U_n] = 2[V_{m+n} + \delta U_{m+n}] , \\ [V_n + \delta U_n]^r = 2^{r-1}[V_{nr} + \delta U_{nr}] , \end{cases}$$

que l'on déduit des relations (6) coïncident avec les formules

$$(\cos x + \sqrt{-1}\sin x)\,(\cos y + \sqrt{-1}\sin y) = \cos (x + y) + \sqrt{-1}\sin (x + y),$$

$$(\cos x + \sqrt{-1}\sin x)^r = \cos rx + \sqrt{-1}\sin rx ,$$

qui ont été données par MOIVRE.

Nous ferons encore observer que si, dans l'équation (1), on pose

$$X = x^r, \qquad \alpha = a^r, \qquad \beta = b^r,$$

les quantités α et β sont les racines de l'équation

$$(8)\qquad X^2 = V_r X - Q^r .$$

Par conséquent, chacune des formules qui appartiennent à la théorie présente peut être généralisée, en y remplaçant U_n et V_n par $\frac{U_{nr}}{U_r}$ et V_{nr}, P par V_r, Q par Q^r, et la différence δ des racines a et b par la différence à δU_r des racines α et β de l'équation (8).

Les formules (4) deviennent ainsi

$$(9)\quad \begin{cases} 2^{n-1}\dfrac{U_{nr}}{U_r} = \dfrac{n}{1}V_r^{n-1} + \dfrac{n(n-1)(n-2)}{1.2.3}\Delta U_r^2 V_r^{n-3} \\ \qquad\qquad + \dfrac{n(n-1)(n-2)(n-3)(n-4)}{1.2.3.4.5}\Delta^2 U_r^4 V_r^{n-5} + \ldots \\ 2^{n-1}V_{nr} = V_r^n + \dfrac{n(n-1)}{1.2}\Delta U_r^2 V_r^{n-2} \\ \qquad\qquad + \dfrac{n(n-1)(n-2)(n-3)}{1.2.3.4}\Delta^2 U_r^4 V_r^{n-4} + \ldots \end{cases}$$

D'ailleur, nous laisserons de côté, pour l'instant, les autres procédés de transformation de l'équation (1) par substitution de variable, ainsi que l'étude des fonctions plus générales

$$AU_n + BV_n + C\ ,$$

dans lesquelles A, B, C désignent des nombres entiers quelconques, positifs ou négatifs.

SECTION III.

Des relations de récurrence pour le calcul des fonctions U_n et V_n.

Le calcul des valeurs de U_n et de V_n qui correspondent aux valeurs entières et consécutives de n, s'éffectue rapidement au moyen de formules entièrement analogues à celles de THOMAS SIMPSON :

$$\sin(n+2)z = 2\cos z \sin(n+1)z - \sin nz\ ,$$

$$\cos(n+2)z = 2\cos z \cos(n+1)z - \cos nz\ .$$

En effet, multiplions par x^n les deux membres de l'équation (1), et remplaçons successivement x par a et b, nous obtenons

$$a^{n+2} = Pa^{n+1} - Qa^n\ , \qquad b^{n+2} = Pb^{n+1} - Qb^n$$

et, par soustraction et par addition,

$$(10)\quad \begin{cases} U_{n+2} = PU_{n+1} - QU_n\ , \\ V_{n+2} = PV_{n+1} - QV_n\ . \end{cases}$$

Ces formules nous font voir que les fonctions U et V forment, pour les valeurs entières et consécutives de n, deux séries récurrentes de nombres entiers. Ces séries ont la même loi de formation, mais elles diffèrent par les conditions initiales. Nous généraliserons ces formules par l'emploi du calcul symbolique. En effet, en désignant par F une fonction quelconque, on tire évidemment de l'équation (1)

$$F(x^2) = F(Px - Q) ;$$

si l'on remplace x par a et b, on a

$$a^n F(a^2) = a^n F(Pa - Q) , \quad b^n F(b^2) = b^n F(Pb - Q) ,$$

et, par soustraction et par addition, on obtient les égalités symboliques

$$(11) \quad \begin{cases} U^n F(U^2) = U^n F(PV - Q) \\ V^n F(V^2) = V^n F(PV - Q) \end{cases}$$

dans lesquelles on remplace, après le développement, les exposants de U et de V par des indices, en tenant compte de l'exposant zéro. Ainsi les symboles U^2 *et* $PU - Q$, V^2 et $PV -$ Q sont respectivement, équivalents, et peuvent être remplacés l'un par l'autre dans les transformations algébriques.

On a, par exemple, dans la série de FIBONACCI, les résultats suivants

$$(12) \quad \begin{cases} u^{n+p} = u^{n-p}(u + 1)^p , \\ u^{n-p} = u^n(u - 1)^p , \end{cases}$$

qui sont entièremont analogues à ceux que l'on peut obtenir dans la théorie des combinaisons ou du triangle arithmétique, et, en particulier dans la formule du binôme des factorielles, due à VANDERMONDE.

En prenant, pour point de départ, l'équation

$$x^2 = x - 1$$

on trouvera encore de nouvelles relations entre les coefficients de la même puissance du binôme

La considération de l'équation (8) conduit aux relations suivantes

$$(13) \quad \begin{cases} U_{n+2r} = V_r U_{n+r} - Q^r U_n , \\ V_{n+2r} = V_r V_{n+r} - Q^r V_n, \end{cases}$$

qui permettent de calculer les valeur des fonctions U_n, et V_n, qui correspondent à des valeurs de l'argument n en progression arithmétique de raison r.

Inversement, on trouvera, dans la théorie des fonctions circulaires et hyperboliques, des formules analogues aux formules (11) et (13).

SECTION IV.

Des relations des fonctions U_n et V_n avec les déterminants.

On peut exprimer U_n *et* U_{nr}, V_n et V_{nr} au moyen de déterminants ; en effet, on a les formules

$$\begin{aligned}
U_2 - PU_1 &= 0\\
U_3 - PU_2 + QU_1 &= 0\\
U_4 - PU_3 + QU_2 \quad * &= 0\\
U_5 - PU_4 + QU_3 - \quad * \quad * &= 0\\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ &\\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ &\\
U_{n+1} - PU_n + QU_{n-1} - \quad * \quad * &= 0
\end{aligned}$$

on en déduit

$$(14)\quad U_{n+1} = (-1)^n \begin{vmatrix} -P, & +1, & 0, & 0, & \cdot & \cdot & \cdot & \cdot \\ +Q, & -P, & +1, & 0, & \cdot & \cdot & \cdot & \cdot \\ 0, & +Q, & -P, & +1, & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & +Q, & -P, & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix} (n \text{ colonnes})$$

On obtient aussi

$$(15)\quad V_n = (+-1)^n \begin{vmatrix} -P, & +2, & 0, & 0, & \cdot & \cdot & \cdot & \cdot \\ +Q, & -P, & +1, & 0, & \cdot & \cdot & \cdot & \cdot \\ 0, & +Q, & -P, & +1, & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & +Q, & -P, & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix} (n \text{ colonnes})$$

On vérifie les résultats que nous venons de trouver, en développant les déterminants suivant les éléments de la derniére ligne ou de la dernière colonne. Les valeurs de $\frac{U_{nr}}{U_r}$ et de V_n, s'obtiennent encore au moyen des déterminants, en remplaçant comme l'ordinaire P par V_r, et Q par Q^r.

Enfin, nous ferons observer que ces formules sont susceptibles d'une grande généralisation ; en effet dans les formules (11) qui contiennent une fonction arbitraire, faisons n successivement égal à $1, 2, 3, \ldots m$; nous obtenons alors m équations desquelles on tirera la valeur de l'une ou de l'autre des fonctions U et V.

REMARQUE, — On peut encore pour le développement de U_n employer la formule suivante,

$$U_{n+1} = \begin{vmatrix} P, & \sqrt{Q}, & 0, & 0, & \ldots \\ \sqrt{Q}, & P, & \sqrt{Q}, & 0, & \ldots \\ 0, & \sqrt{Q}, & P, & \sqrt{Q}, & \ldots \\ 0, & 0, & \sqrt{Q}, & P, & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{vmatrix} \quad (n \text{ colonnes}) \tag{16}$$

Cependant l'emploi de la formule (14) est bien préférable.

SECTION V.

Des relations des fonctions U_n et V_n avec les fractions continues.

Les fonctions U_n et V_n sont développables en fractions continues ; en effet, considérons l'expression

$$\frac{R_n}{S_n} = a_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \ldots}}} \qquad + \frac{a_n}{b_n}, \tag{17}$$

et désignons par R_n et S_n, le numérateur et le dénominateur de la $n^{ième}$ réduite ; on sait que l'on a

$$\begin{cases} R_{n+2} = b_{n-2}R_{n+1} + a_{n+2}R_n, \\ S_{n+2} = b_{n+2}S_{n+1} + a_{n+2}S_n ; \end{cases} \tag{18}$$

et, de plus

$$R_nS_{n+1} - R_{n+1}S_n = (-1)^n a_1\, a_2\, a_2 \ldots a_{n+1}. \tag{19}$$

Par conséquent, si l'on pose

$$a_0 = b_1 = b_2 = \ldots = b_n = P,$$
$$a_1 = a_2 = a_3 = \ldots = a_n = -Q,$$

on obtient l'expression

$$\frac{U_{n+1}}{U_n} = P - \cfrac{Q}{P - \cfrac{Q}{P - \cfrac{Q}{P - \ldots}}} \tag{20}$$

.

dans laquelle n désigne le nombre des quantités égales à P.

On a ainsi, dans la série de FIBONACCI :

$$\frac{1}{2}\frac{(1+\sqrt{5})^{n+1}-(1-\sqrt{5})^{n+1}}{(1+\sqrt{5})^{n}-(1-\sqrt{5})^{n}}=1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+.}}} \qquad (21)$$

.

dans la série de FERMAT :

$$\frac{2^{n+1}-1}{2^{n}-1}=3-\cfrac{2}{3-\cfrac{2}{3-\cfrac{2}{3-.}}} \qquad (22)$$

.

.

et dans la série de PELL

$$\frac{1}{2}\frac{(1+\sqrt{2})^{n+1}-(1-\sqrt{2})^{n+1}}{(1+\sqrt{2})^{n}-(1-\sqrt{2})^{n}}=2-\cfrac{1}{2-\cfrac{1}{2-\cfrac{1}{2-.}}} \qquad (23)$$

.

.

D'ailleurs, on a généralement

$$\frac{U_{n+1}}{U_n}=a\frac{1-\left(\frac{b}{a}\right)^{n+1}}{1-\left(\frac{b}{a}\right)^{n}} \ ; \qquad (24)$$

donc, en désignant par a la plus grande des racines, prises en valeur absolue, de l'équation (1), on a

$$\operatorname{Lim}\frac{U_{n+1}}{U_n}=a\,, \qquad (25)$$

lorsque n augmente indéfiniment. Cependant, nous ferons observer que ce dernier résultat ne s'applique pas dans le cas des séries de troisième espèce, c'est-à-dire lorsque les racines de l'équation proposée (1) sont imaginaires.

Au moyen de cette dernière formule, il est facile de calculer rapidement un terme de la série U_n lorsque l'on ne connait que le précèdent. Soit, par exemple, dans la série de FIBONACCI

$$u_{44} = 7014\ 08733,$$

et

$$a = \frac{1+\sqrt{5}}{2} = 1,\ 61803\ 39887\ 39894\ 8482\ \ldots\ ;$$

si l'on calcule par les méthodes abrégées le produit $a.u_{44}$, à moins d'une unité près, on trouve exactement, puisque u_n, est entier

$$u_{45} = 11349\ 03170.$$

On peut, d'ailleurs, déterminer directement le dernier chiffre de u_n ; ainsi dans ce cas particulier, il est facile de faire voir que deux termes, dont les rangs, différent d'un multiple quelconque de 60, sont terminés par le même chiffre ; si l'on suppose alors p intérieur à 60, on peut démontrer que les derniers chiffres de u_p et de u_q, sont complémentaires, lorsque la somme $p + q$ est égale à 60 ; on peut donc supposer maintenant p égal à 30 ; et même p inférieur à 15, si l'on observe que les termes u_{15+p} et u_{15-p} ont les mêmes derniers chiffres, lorsque p est impair, et leurs derniers chiffres complémentaires, lorsque p est pair.

On a, plus généralement, la formule

$$\frac{U_{(n+1)r}}{U_{nr}} = V_r - \cfrac{Q^r}{V_r - \cfrac{Q^r}{V_r - \cfrac{Q^r}{V_r - \ddots}}} \qquad (26)$$

dans laquelle les V_r sont en nombre n, et, lorsque n augmente indéfiniment,

$$\operatorname{Lim} \frac{U_{(n+1)r}}{U_r} = a^r\ . \qquad (27)$$

A la formule (26), correspond, dans la théorie des fonctions circulaires la formule*

$$\frac{\sin(n+1)z}{\sin nz} = 2\cos z - \cfrac{1}{2\cos z - \cfrac{1}{2\cos z - \cfrac{1}{2\cos z - \ddots}}} \qquad (28)$$

dans laquelle l'expression $2\cos z$ est répétée n fois ;

* Journal de Crelle, tome xvi, pag. 95 ; 1887

On a aussi pour la série des V_n, la relation

$$(29)\qquad \frac{V_{nr}}{V_{n-1r}} = V_r - \cfrac{Q^r}{V_r - \cfrac{Q^r}{V_r - \cfrac{Q^r}{V_r - .}}} \; . - \frac{Q^r}{\left(\frac{V_r}{2}\right)},$$

dans laquelle la quantité V_r est répétée n fois.

Les nombreuses propriétiés des déterminants et des fractions continues donnent lieu à des propriétés analogues pour les fonctions U_n et V_n. Ainsi la propriété bien connue de deux réduites consécutives, renfermée dans la formule (19) donne

$$(30)\qquad \begin{cases} U_n^2 - U_{n-1}U_{n+1} = Q^{n-1}, \\ V_n^2 - V_{n-1}V_{n+1} = -Q^{n-1}\Delta, \end{cases}$$

et, plus généralement

$$(31)\qquad \begin{cases} U_{nr}^2 - U_{(n-1)r}U_{(n+1)r} = Q^{(n-1)r}U_r^2, \\ V_{nr}^2 - V_{(n-1)r}V_{(n+1)r} = -Q^{(n-1)r}\Delta U_r^2 \; ; \end{cases}$$

on a, dans la théorie des fonctions circulaires, les formules analogues

$$\sin^2 x - \sin(x-y)\sin(x+y) = \sin^2 y,$$
$$\cos^2 x - \cos(x-y)\cos(x+y) = \sin^2 y,$$

Il est d'ailleurs facile de vérifier immédiatement les formules (31), en remplaçant U, V et Q en fonction de a et b. Ainsi, on a encore

$$\Delta U_{n+r}^2 = a^{2n+2r} + b^{2n+2r} - 2Q^{n+r},$$
$$\Delta U_n^2 \;\; = a^{2n} \;\;\; + b^{2n} \;\;\; - 2Q^n \;\; ;$$

donc, par soustraction :

$$\Delta\left[U_{n+r}^2 - Q^r U_n^2\right] = \left[a^{2n+r} - b^{2n+r}\right]\left[a^r - b^r\right],$$

et, par suite

$$(32)\qquad U_{n+r}^2 - Q^r U_n^2 = U_r U_{2n+r} \; ;$$

on aura, par la même voie, la relation

$$(33)\qquad V_{n+r}^2 - Q^r V_n^2 = \Delta U_r U_{2n+r} \; ,$$

La formule (32) donne plus particulièrement, pour $r = 1$, la relation

$$(34)\qquad U_{n+1}^2 - QU_n^2 = U_{2n+1} \; .$$

Cette dernière formule a été appliquée par M. GÜNTHER, à la résolution de l'équation indéterminée

$$y^2 - Qx^2 = Kz ,$$

en nombres entiers[*] ; il est facile de voir qu'un très-grand nombre de formules de cette section et des suivantes, conduisent à des conséquences analogues, mais beaucoup plus générales.

SECTION VI.

Développement des fonctions U_n et V_n en séries de fractions.

Les formules (30) donnent lieu aux développements de $\frac{U_{n+1}}{U_n}$ et $\frac{V_{n+1}}{V_n}$ en séries dont les termes ont pour dénominateurs le produit de deux termes consécutifs des séries U et V. On a, en effet,

$$\frac{U_{n+1}}{U_n} = \frac{U_2}{U_1} + \left(\frac{U_3}{U_2} - \frac{U_2}{U_1}\right) + \left(\frac{U_4}{U_3} - \frac{U_3}{U_2}\right) + \ldots . + \left(\frac{U_{n+1}}{U_n} - \frac{U_n}{U_{n-1}}\right) ,$$

et, en réunissant les fractions contenues dans chaque parenthèse,

$$\frac{U_{n+1}}{U_n} = \frac{U_2}{U_1} - \frac{Q}{U_1U_2} - \frac{Q^2}{U_2U_3} - \frac{Q^3}{U_3U_4} - \ldots . - \frac{Q_{n-1}}{U_{n-1}U_n} ; \tag{35}$$

on a ainsi dans la série de FIBONACCI, pour augmentant indéfiniment

$$\frac{1+\sqrt{5}}{2} = 1 + \frac{1}{1.1} - \frac{1}{1.2} + \frac{1}{2.3} - \frac{1}{3.5} + \frac{1}{5.8} - \frac{1}{8.13} + \ldots . \tag{36}$$

En suivant la même voie, on obtient les formules plus générales

$$\frac{U_{(n+1)r}}{U_{nr}} = \frac{U_{2r}}{U_r} - \left[\frac{Q^r}{U_rU_{2r}} + \frac{Q^{2r}}{U_{2r}U_{3r}} + \ldots . + \frac{Q^{(n-1)r}}{U_{(n-1)r}U_{nr}}\right] U_r^2 , \tag{37}$$

et

$$\frac{V_{(n+1)r}}{V_{nr}} = \frac{V_r}{V_0} - \left[\frac{Q^r}{V_0V_r} + \frac{Q^{2r}}{V_rV_{2r}} + \ldots . + \frac{Q^{nr}}{V_{(n-1)r}V_{nr}}\right] \Delta U_r^2 . \tag{38}$$

On tire encore des deux relations

$$\begin{cases} U_{n+r}V_n - U_nV_{n+r} = 2Q^nU_r , \\ V_{n+r}V_n - \Delta U_nU_{n+r} = Q^nV_r , \end{cases} \tag{39}$$

---

[*] *Journal de Mathématiques pures et appliquées,* de M. RESAL, pag. 331-341 ; Octobre, 1876. Vol. I – n°. 3.-50.

que nous démontrerons plus loin, les développements

$$(40)\qquad \begin{cases} \dfrac{U^{n+kr}}{V_{n+kr}} = \dfrac{U_n}{V_n} + 2Q^n U_r \left[\dfrac{1}{V_r V_{n+r}} + \dfrac{Q^r}{V_{n+r} V_{n+2r}} + \ldots . + \dfrac{Q^{(k-1)r}}{V_{n+(k-1)r} V_{n+kr}} \right], \\ \dfrac{V^{n+kr}}{U_{n+kr}} = \dfrac{V_n}{U_n} - 2Q^n U_r \left[\dfrac{1}{U_r U_{n+r}} + \dfrac{Q^r}{U_{n+r} U_{n+2r}} + \ldots . + \dfrac{Q^{(k-1)r}}{U_{n+(k-1)r} U_{n+kr}} \right]. \end{cases}$$

Lorsque k augmente indéfiniment, les premiers membres des égalités précédentes ont respectivement pour limites $\dfrac{1}{\sqrt{\Delta}}$ et $\sqrt{\Delta}$; on tiendra compte dans le second membre, des conditions de convergence.

On peut ainsi développer la racine carrée d'un nombre entier en séries de fractions ayant pour numérateur l'unité ; c'était un usage familier aux savants de la Grèce et de l'Égypte ; ainsi, par exemple, cette valeur approximative de

$$\frac{\sqrt{3}}{4} = \frac{1}{3} + \frac{1}{10} + \varepsilon ,$$

rapportée par COLUMELLE au chapitre V de son ouvrage *de Rê Rusticâ* ; ainsi encore, cette valeur approximative de

$$\sqrt{2} = 1 + \frac{1}{3} + \frac{1}{3.4} - \frac{1}{12.34} + \varepsilon ,$$

donnée par les auteurs indiens BAUDHAYANA et APASTAMBA[*] ; cette valeur approximative est égale au rapport des termes $V_8 = 577$ et $U_8 = 408$, de la série de PELL.

SECTION VII. .

Des relations des fonctions U_n et V_n avec la théorie de la divisibilité.

Si nous posons $\alpha = a^r$ et $\beta = b^r$, et, par suite, $\alpha\beta = Q^r$, nous obtenons, par la formule qui donne le quotient de $\alpha^n - \beta^n$ par $\alpha - \beta$, les résultats suivants :

1°. Lorsque n désigne un nombre *pair* :

$$(41)\qquad \frac{U_{nr}}{U_r} = V_{(n-1)r} + Q^r V_{(n-3)r} + Q^{2r} V_{(n-5)r} + \ldots . + Q^{\left(\frac{n}{2}-1\right)r} V_r \ ;$$

2°. Lorsque n désigne un nombre *impair* :

$$(42)\qquad \frac{U_{nr}}{U_r} = V_{(n-1)r} + Q^r V_{(n-3)r} + Q^{2r} V_{(n-5)r} + \ldots . + Q^{\left(\frac{n-1}{2}\right)r} V_r \ ;$$

[*] *The Çulvasûtras* by G. THIBAUT, pag. 13-15. *Journal of the Asiatic Society of Bengal*, 1875.

Le quotient de $\alpha^n - \beta^n$ par $\alpha + \beta$, lorsque n désigne un nombre *pair*, donne encore

$$\frac{U_{nr}}{V_r} = U_{(n-1)r} - Q^r U_{(n-3)r} + Q^{2r} U_{(n-5)r} - \ldots + (-Q^r)^{\frac{n}{2}-1} U_r \ , \tag{43}$$

et le quotient de $\alpha^n + \beta^n$ par $\alpha + \beta$, lorsque n désigne un nombre *impair*, donne enfin

$$\frac{V_{nr}}{V_r} = V_{(n-1)r} - Q^r V_{(n-3)r} + Q^{2r} V_{(n-5)r} - \ldots + (-Q^r)^{\frac{n-1}{2}} \ . \tag{44}$$

Pour n = 2, on retrouve la formule

$$U_{2r} = U_r V_r \ , \tag{3}$$

et, pour $n = 3$, on a

$$\begin{cases} U_{3r} = U_r \ (\ V_{2r} + Q^r \ ) \ , \\ V_{3r} = V_r \ (\ V_{2r} - Q^r \ ) \ . \end{cases} \tag{45}$$

Les relations précédentes nous montrent que U_m est toujours divisible par U_n, lorsque m est divisible par n ; de même V_m est toujours divisible par V_n, lorsque m est impair et divisible par n ; par conséquent U_m et V_m ne peuvent être des nombres premiers, que si m est premier ; mais la réciproque de ce théorème n'a pas lieu.

Dans la série de FIBONACCI, u_3 est divisible par 2, u_4 est divisible par 3, u_5 est divisible par 5 ; par conséquent, u_{3n}, u_{4n} et u_{5n}, sont respectivement divisibles par 2, 3, et 5. Ainsi encore, bien que 53 soit premier on a

$$u_{53} = 953 \times 559\,45741.$$

Reprenons les égalités

$$V_n + \delta U n = 2a^n \ , \qquad V_n - \delta U n = 2b^n \ ; \tag{6}$$

nous obtenons, en multipliant membre à membre, la relation

$$V_n^2 - \Delta U_n^2 = 4Q^n \ , \tag{46}$$

qui correspond, en trigonométrie, à la formule

$$\cos^2 z + \sin^2 z = 1.$$

Cette relation nous montre que si U_n et V_n admettaient un diviseur commun θ, ce diviseur serait un facteur de Q ; mais, d'autre part,

$$V_n = \left(\frac{P+\delta}{2} \right)^n + \left(\frac{P-\delta}{2} \right)^n ,$$

et, en supprimant les multiples de Q, ce qui revient évidemment à remplacer δ par Q, on a la congruence.

$$V_n \equiv P^n , \qquad (\text{Mod. } Q) \ ; \tag{47}$$

donc, tout diviseur θ de U_n et V_n diviserait P et Q ; or nous avons supposé premiers entre eux. De là résulte cette proposition :

THEOREME : *Les nombres U_n et V_n sont premiers entre eux.*

Si l'on désigne par μ l'exposant auquel appartient P suivant le module Q, on sait que la congruence

$$P^n \equiv 1, \quad (\text{Mod. } Q),$$

est vérifiée pour toutes les valeurs de n égales à un multiple quelconque de μ, μ étant lui-même un certain diviseur de l'indicateur $\phi(Q)$ de Q, ou du nombre des entiers inférieurs et premiers à Q ; par conséquent, à cause de l'égalité (47), on résoudra la congruence

$$V_n \equiv 1, \quad (\text{Mod. } Q), \tag{48}$$

par toutes les valeurs de n égales à un multiple quelconque de μ.

SECTION VIII.

Des formes linéaires et quadratiques des diviseurs de U_n et V_n, qui correspondent aux valeurs paires et impaires de l'argument n.

La formule (46) conduit encore à d'autres conséquences importantes sur la forme des diviseurs de U_n et de V_n, car on en déduit immédiatement les propositions suivantes, suivant que l'on considère n égal à un nombre pair ou à un nombre impair.

THEOREME : *Les termes de rang impair de la serie U_n sont des diviseurs de la forme quadratique $x^2 - Qy^2$.*

En tenant compte des résultats bien connus de la théorie des diviseurs des formes quadratiques, on a, en particulier, pour les formes linéaires correspondantes des diviseurs premiers impairs de U_{2r+1}

dans la série de	FIBONACCI :	$4q + 1$;
” ”	FERMAT:	$8q + 1, 7$;
” ”	PELL :	$4q + 1$.

Ainsi, les termes de rang impair de la série de FIBONACCI ou de la série de PELL ne peuvent contenir comme diviseur aucun nombre premier de la forme $4q + 3$.

THEOREME : *Les termes de rang pair de la série V_n sont des diviseurs de la forme quadratique $x^2 + \Delta y^2$.*

En particulier, les formes linéaires correspondantes des diviseurs premiers impairs de V_{2r} sont

dans la série de FIBONACCI : $20q + 1, 3, 7, 9$;
" " FERMAT : $4q + 1$;
" " PELL : $8q + 1, 3$.

THEOREME : *Les termes de rang impair de la série* V_n *sont des diviseurs de la forme quadratique* $x^2 + Q\delta y^2$.

En particulier, les formes linéaires correspondantes des diviseurs premiers impairs de V_{2r+1} sont

dans la série de FIBONACCI : $20q + 1, 9, 11, 19$;
" " FERMAT : $8q + 1, 3$;
" " PELL : $8q + 1, 7$.

SECTION IX.

Des formules concernant l'addition des fonctions numériques.

En multipliant membre à membre les relations

$$V_m + \delta U_m = 2a^m \qquad V_n + \delta U_n = 2a^n ,$$

on obtient,

$$V_m V_n + \Delta U_m U_n + \delta[U_m V_n + U_n V_m] = 4a^{m+n} ;$$

si l'on change a en b, et δ en $-\delta$, on déduit ensuite par addition et par soustraction, les formules

$$(49) \quad \begin{cases} 2U_{m+n} = U_m V_n + U_n V_m , \\ 2V_{m+n} = V_m U_n + \Delta U_m U_n , \end{cases}$$

auxquelles correspondent en trigonométrie les formules de l'addition des arcs :

$$\sin(x + y) = \sin x \cos y + \sin y \cos x ,$$
$$\cos(x + y) = \cos x \cos y - \sin x \sin y .$$

Si nous changeons n en $-n$ dans les formules (49), en tenant compte des relations

$$(50) \qquad U_{-n.} = -\frac{U_n}{Q^n} , \qquad V_{-n} = \frac{V_n}{Q^n} ,$$

nous obtenons

$$(51) \quad \begin{cases} 2Q^n U_{m-n} = U_m V_n - U_n V_m , \\ 2Q^n V_{m-n} = V_m U_n - \Delta U_m U_n ; \end{cases}$$

en faisant $m = n + r$, on obtient les formules (39) données plus haut.

La comparaison des égalités (49) et (51) nous donne immédiatement

$$U_{m+n} + Q^n U_{m-n} = U_m V_n \ ,$$
$$U_{m+n} - Q^n U_{m-n} = U_n V_m \ ;$$

posons maintenant

$$m + n = r, \qquad m - n = s \ ,$$

il vient

$$(52) \quad \begin{cases} U_r + Q^{\frac{r-s}{2}} U_s = U_{\frac{r+s}{2}} V_{\frac{r-s}{2}} \ , \\ U_r - Q^{\frac{r-s}{2}} U_s = U_{\frac{r-s}{2}} V_{\frac{r-s}{2}} \ ; \end{cases}$$

ces relations sont entièrement semblables à celles qui permettent de transformer la somme ou la différence de deux lignes trigonométriques, en un produit. On a, de même

$$(53) \quad \begin{cases} V_r + Q^{\frac{r-s}{2}} V_s = V_{\frac{r+s}{2}} V_{\frac{r-s}{2}} \ , \\ V_r - Q^{\frac{r-s}{2}} V_s = \Delta U_{\frac{r+s}{2}} U_{\frac{r-s}{2}} \ . \end{cases}$$

On aura encore, comme pour la somme des sinus ou des cosinus d'arcs en progression arithmétique

$$(54) \quad \begin{cases} U_m + Q^{\frac{-r}{2}} U_{m+r} + Q^{\frac{-2r}{2}} U_{m+2r} + \ldots + Q^{\frac{-nr}{2}} U_{m+nr} = U_{\frac{2m+nr}{2}} \dfrac{U_{\frac{n+1}{2}r} Q^{\frac{m}{4}}}{U_{\frac{r}{2}} Q^{\frac{nr}{2}}} \ , \\ V_m + Q^{\frac{-r}{2}} V_{m+r} + Q^{\frac{-2r}{2}} V_{m+2r} + \ldots + Q^{\frac{-nr}{2}} V_{m+nr} = V_{\frac{2m+nr}{2}} \dfrac{U_{\frac{n+1}{2}r} Q^{\frac{m}{4}}}{U_{\frac{r}{2}} Q^{\frac{nr}{2}}} \ ; \end{cases}$$

et, par suite

$$(55) \quad \frac{U_m + Q^{\frac{-r}{2}} U_{m+r} + Q^{\frac{-2r}{2}} U_{m+2r} + \ldots + Q^{\frac{-nr}{2}} U_{m+nr}}{V_m + Q^{\frac{-r}{2}} V_{m+r} + Q^{\frac{-2r}{2}} V_{m+2r} + \ldots + Q^{\frac{-nr}{2}} V_{m+nr}} = \frac{U_{m+\frac{n}{2}r}}{V_{m+\frac{n}{2}r}} \ .$$

On trouve des formules beaucoup plus simples en partant des relations

$$(13) \quad \begin{cases} U_{n+2r} = V_r U_{n+r} - Q^r U_n \ , \\ V_{n+2r} = V_r V_{n+r} - Q^r V_n \ ; \end{cases}$$

si l'on remplace successivement n par 0, r, $2r$, ... $(n-1)r$, et si l'on ajoute, on obtient

$$(56) \quad \begin{cases} U_r + U_{2r} + \ldots + U_{nr} = \dfrac{U_r + Q^n U_{nr} - U_{(n+1)r}}{1 + Q^r - V_r} \ , \\ V_r + V_{2r} + \ldots + V_{nr} = \dfrac{V_r + Q^n V_{nr} - V_{(n+1)r}}{1 + Q^r - V_r} \ . \end{cases}$$

Ces formules se présentent sous une forme indéterminée lorsque le dénominateur s'annule, c'est-à-dire pour

$$1 + a^r b^r - a^r - b^r = 0 ,$$

ou bien

$$(1 - a^r)\,(1 - b^r) = 0 ;$$

c'est-à-dire pour les valeurs de a ou de b égales à l'unité ; dans ce cas, on emploie le procédé de sommation de la progression géometrique. On a d'ailleurs, dans la série de FIBONACCI, pour $r = 1$ et $r = 2$,

$$u_1 + u_2 + u_3 + \ldots + u_n = u_{n+2} - 1 ,$$
$$u_2 + u_4 + u_6 + \ldots + u_{2n} = u_{2n+1} - 1 ,$$
$$v_1 + v_2 + v_3 + \ldots + v_n = v_{n+2} - 3 ,$$
$$v_2 + v_4 + v_6 + \ldots + v_{2n} = v_{2n+1} - 1 ,$$

On trouvera encore plus généralement,

$$(57) \qquad U_{m+r} + U_{m+2r} + U_{m+3r} + \ldots + U_{m+nr} = \frac{U_{m+r} + Q^r U_{m+nr} - U_{m+(n+1)r} - Q^r U_m}{1 + Q^r - V_r} ,$$

et un résultat analogue en changeant U en V.

La formule d'addition peut s'écrire encore

$$2\frac{U_{m+n}}{U_n} = \frac{U_m}{U_n} V_n + V_m ;$$

on a, par conséquent

$$(58) \qquad 2\frac{U_{m+n} U_{m+n-1} \ldots U_{m+1}}{U_n\, U_{n-1} \ldots U_1} = \frac{U_{m+n-1} U_{m+n-2} \ldots U_m}{U_n\, U_{n-1} \ldots U_1} V_n + \frac{U_{m+n-1} U_{m+n-2} \ldots U_{m+1}}{U_{n-1} U_{n-2} \ldots U_1} V_m .$$

On en déduit immédiatement cette proposition :

THEOREME : *Le produit de n termes consécutifs de la série U_n est divisible par le produit des n premiers termes.*

Nous terminerons ce paragraphe par la démonstration de formules d'une extrême importance ; car elles nous serviront ultérieurement comme base de la théorie des fonctions numériques doublement périodiques, déduites de la considération des fonctions symétriques des racines des équations du troisième et du quatrième degré à coefficients commensurables. Les formules (30) nous donnent

$$U_{m-1} U_{m+1} = U_m^2 - {}^{m-1}Q,$$
$$U_{n-1} U_{n+1} = U_n^2 - {}^{n-1}Q ;$$

on en déduit

$$U_n^2 U_{m-1} U_{m+1} - U_m^2 U_{n-1} U_{n+1} = Q^{n-1}\left[U_m^2 - Q^{m-n} U_n^2\right] ,$$

et, par les formules (32)

(*A*) $$U_n^2 U_{m-1} U_{m+1} - U_m^2 U_{n-1} U_{n+1} = Q^{n-1} U_{m-n} U_{m+n} \ ;$$

on a, de même

(*A'*) $$V_n^2 V_{m-1} V_{m+1} - V_m^2 V_{n-1} V_{n+1} = -\Delta Q^{n-1} V_{m-n} V_{m+n} \ .$$

En particulier, pour $m = n + 1$, et pour $m = n + 2$, on a

(*B*) $$\begin{cases} U_n^3 U_{n+2} - U_{n+1}^3 U_{n-1} = Q^{n-1} U_{2n+1} \ , \\ U_n^2 U_{n+1} U_{n+3} - U_{n+2}^2 U_{n-1} U_{n+1} = Q^{n-1} U_2 U_{2n+2} \ , \end{cases}$$

Et des formules analogues pour les V_n.

Les formules (*A*) et (*B*) appartiennent à la théorie des fonctions elliptiques, et, plus spécialement, aux fonctions que JACOBI a désignées par les symboles Θ et H.

SECTION X.

De la somme des carrés des fonctions numériques U_n et V_n .

Si dans la relation suivante

(59) $$\Delta U_{r+2x\rho} U_{s+2x\sigma} = V_{r+s+2x(\rho+\sigma)} - Q^{s+2x\sigma} V_{r-s+2x(\rho-\sigma)} \ ,$$

nous supposons successivement x égal à 0, 1, 2, 3, . *n*, et si nous ajoutons membre à membre les égalités obtenues, après avoir divisé respectivement par

$$1, \ Q^{\rho+\sigma}, \ Q^{2(\rho+\sigma)}, \ . \ . \ . \ . \ Q^{n(\rho+\sigma)}, \ . \ .$$

nous obtenons la formule

$$(60) \sum_{x=0}^{x=n} U_{r+2x\rho} U_{s+2x\sigma} = \frac{U_{r+2n\rho} U_{s+(2n+1)\sigma} - Q^{\sigma-\rho} U_{r+(2n+1)\rho} U_{s+2n\sigma}}{\Delta Q^{n(\rho+\sigma)} U_{\sigma-\rho} U_{\sigma+\rho}} + \frac{U_r U_{s-2\sigma} - Q^{\sigma-\rho} U_{r-2\rho} U_s}{\Delta U_{\sigma-\rho} U_{\sigma+\rho}} ,$$

en particulier, pour $2\rho = r$ et $2\sigma = s$,

$$(61) U_r U_s + \frac{U_{2r} U_{2s}}{Q^{\frac{r+s}{2}}} + \frac{U_{3r} U_{3s}}{Q^{r+s}} + \ldots + \frac{U_{(n+1)r} U_{(n+1)s}}{Q^{\frac{n}{2}(r+s)}} = \frac{U_{(n+1)r} U_{2(n+1)s} - Q^{\frac{s-r}{2}} U_{(n+1)s} U_{2(n+1)r}}{\Delta Q^{\frac{n}{2}(r+s)} U_{\frac{s-r}{2}} U_{\frac{s+r}{2}}} ,$$

et, plus particuliérement encore

$$(62)\quad \begin{cases} \dfrac{U_r^2}{Q^r}+\dfrac{U_{2r}^2}{Q^{2r}}+\dfrac{U_{3r}^2}{Q^{3r}}+\ldots+\dfrac{U_{(n+1)r}^2}{Q^{(n+1)r}}=\dfrac{1}{\Delta}\left[\dfrac{U_{(2n+3)r}}{U_rQ^{(n+1)r}}-2n-3\right], \\ \dfrac{U_r^2}{Q^r}+\dfrac{U_{3r}^2}{Q^{3r}}+\dfrac{U_{5r}^2}{Q^{5r}}+\ldots+\dfrac{U_{(2n+1)r}^2}{Q^{(2n+1)r}}=\dfrac{1}{\Delta}\left[\dfrac{U_{4(n+1)r}}{U_{2r}Q^{(2n+1)r}}-2n-2\right]. \end{cases}$$

Par un procédé analogue, on trouvera aussi les valeurs de

$$\sum_{x=0}^{x=n}\frac{V_{r+2x\rho}V_{s+2x\sigma}}{Q^{x(\rho+\sigma)}} \quad \text{et de} \quad \sum_{x=0}^{x=n}\frac{U_{r+2x\rho}V_{s+2x\sigma}}{Q^{x(\rho+\sigma)}}$$

En particulier

$$(63)\quad \begin{cases} \dfrac{V_r^2}{Q^r}+\dfrac{V_{2r}^2}{Q^{2r}}+\dfrac{V_{3r}^2}{Q^{3r}}+\ldots+\dfrac{V_{nr}^2}{Q^{nr}}=2n-1+\dfrac{U_{(2n+1)r}}{U_rQ^{nr}}, \\ \dfrac{V_r^2}{Q^r}+\dfrac{V_{3r}^2}{Q^{3r}}+\dfrac{V_{5r}^2}{Q^{5r}}+\ldots+\dfrac{V_{(2n+1)r}^2}{Q^{(2n+1)r}}=2n+2+\dfrac{U_{4(n+1)r}}{U_rQ^{(2n+1)r}}. \end{cases}$$

On a aussi, dans le cas général,

$$(64)\quad \begin{cases} \displaystyle\sum_{x=0}^{x=n}U_{m+xr}^2=\frac{V_{2m+2(n+1)r}-V_{2m}-Q^{2r}\left[V_{2m+2nr}-V_{2m-2r}\right]}{\Delta(V_{2r}-Q^{2r}-1)}-2Q^m\frac{Q^{(n+1)r}-1}{\Delta(Q^r-1)} \\ \displaystyle\sum_{x=0}^{x=n}V_{m+xr}^2=\frac{V_{2m+2(n+1)r}-V_{2m}-Q^{2r}\left[V_{2m+2nr}-V_{2m-2r}\right]}{V_{2r}-Q_{2r}-1}+2Q^m\frac{Q^{(n+1)r}-1}{Q^r-1} \end{cases}$$

On a, par exemple, dans la série de FIBONACCI

$$(65)\quad \begin{cases} u_r^2-u_{2r}^2+u_{3r}^2-\ldots-(-1)^{nr}u_{nr}^2=\dfrac{1}{5}\left[2n+1-(-1)^{nr}\dfrac{u_{(2n+1)r}}{u_r}\right], \\ u_r^2+u_{3r}^2+u_{5r}^2-\ldots+u_{(2n+1)r}^2=\dfrac{1}{5}\left[\dfrac{u_{4(n+1)r}}{u_{2r}}-(-1)^{nr}(2n+2)\right], \\ v_r^2-v_{2r}^2+v_{3r}^2-\ldots-(-1)^{nr}v_{nr}^2=2n-1-(-1)^{nr}\dfrac{u_{(2n+1)r}}{u_r}, \\ v_r^2+v_{3r}^2+v_{5r}^2-\ldots+v_{(2n+1)r}^2=\dfrac{u_{4(n+1)r}}{u_{2r}}-(-1)^{nr}(2n-2)\ ; \end{cases}$$

la formule plus simple

$$(66)\qquad u_1^2+u_2^2+u_3^2+\ldots+u_n^2=u_n\,u_{n+1}\ ,$$

donne ainsi, pour le côté du décagone régulier étoilé, cette expression

$$(67)\qquad \frac{1+\sqrt{5}}{2}=1+\frac{1}{1^2}-\frac{1}{1^2+1^2}+\frac{1}{1^2+1^2+2^2}-\frac{1}{1^2+1^2+2^2+3^2}+\frac{1}{1^2+1^2+2^2+3^2+5^2}-\ldots.$$

On a encore, dans cette série

$$(68)\quad \begin{cases} u_1u_2 + u_2u_3 + u_3u_4 + \ldots + u_{2n-1}u_{2n} = u_{2n}^2 \ , \\ u_1u_2 + u_2u_3 + u_3u_4 + \ldots + u_{2n}u_{2n+1} = u_{2n+1}^2 - 1 \ . \end{cases}$$

SECTION XI.

Des relations des fonctions U_n et V_n avec la théorie du plus grand commun diviseur.

Nous avons trouvé la formule

$$2\ U_{m+n} = U_mV_n + U_nV_m \ .$$

par conséquent, si un nombre impair quelconque θ divise U_{m+n} et U_m, il divise U_nV_m ; mais nous avons démontré (§ 17) que U_m et V_m sont premiers entre eux ; donc θ ,divise U_n. Inversement, tout nombre impair qui divise U_n et U_m divise U_{m+n} ; donc, en ne tenant pas compte du facteur 2, on a cette proposition fondamentale :

THEOREME: *Le plus grand commun diviseur de U_m et de U_n est égal à U_D , en désignant par D le plus grand commun diviseur de m et de n.*

En particulier, les termes U_m et U_n sont premiers entre eux lorsque m et n sont premiers entre eux, car U_1 est égal à l'unité. On déduit d'ailleurs du théorème fondamental un grand nombre de propositions entièrement semblables à celles que l'on obtient dans la théorie du plus grand commun diviseur et du plus petit multiple commun de plusieurs nombres donnés.

Il résulte encore de ce qui précède que, dans la recherche du plus grand commun diviseur de deux termes U_m et U_n , les restes successifs forment aussi des termes de la série ; en particulier, les restes successifs de deux termes consécutifs donnent, dans le cas de Q négatif, tous les termes de la série décroissante, à partir du plus petit d'entre eux. LAME [*] a observé que, dans la recherche du plus grand commun diviseur de deux nombres quelconques, le nombre des restes est au plus égal au nombre des termes de la série de FIBONACCI, inférieurs au plus petit des deux nombres donnés, et il en a déduit ce théorème :

Le nombre des divisions à effectuer dans la recherche du plus grand commun diviseur de deux nombres donnés est au plus égal, dans le système ordinaire de numération, à cinq fois le nombre des chiffres du plus petit des deux nombres donnés.

[*] Comptes rendus de l'Académie des Sciences de Paris, t. xix, pag. 868. Paris, 1844.

On trouverait une limite plus rapprochée, en calculant par logarithmes le rang du terme de la série de FIBONACCI immédiatement inférieur au plus petit des nombres donnés. On voit aisément qu'il suffirait, en désignant ce plus petit nombre par A, de prendre le plus petit entier contenu dans la fraction

$$\frac{\log A+\log\sqrt{5}}{\log\frac{1+\sqrt{5}}{2}}=\frac{\log A+0.349}{0.209}\ .$$

Mais il est préférable de s'en tenir à la limite donnée par l'élégant théorème que nous venons de rappeler.

SECTION XII.

De la multiplication des fonctions numériques.

On peut exprimer les valeurs de U_n et V_n qui correspondent à toutes les valeurs entières et positives de n, en fonction des valeurs initiales ; en effet, on a successivement, pour U, par exemple,

$$(69)\quad \begin{cases} U_2 = PU_1 - QU_0\ , \\ U_3 = (P^2 - Q)U_1 - QPU_0\ , \\ U_4 = (P^3 - 2PQ)U_1 - Q(P^2 - Q)U_0\ , \\ U_5 = (P^4 - 3P^2Q + Q^2)U_1 - Q(P^3 - 2PQ)U_0\ , \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

On observera d'abord que si ϕ_n désigne le coefficient de U_n dans U_{n+1} on a en général,

$$U_{n+1} = \phi_n U_1 - Q\phi_{n-1}U_0$$

Le coefficient ϕ_{n-1} est une fonction homogène et de degré n, de P et de Q, en y considérant P au premier degré et Q au second. Si l'on forme le tableau des coefficients de ϕ_n, on retrouve aisément le triangle arithmétique, mais dans une disposition spéciale. On a d'ailleurs, ainsi qu'on peut le vérifier *a posterori*

$$(70)\quad \begin{cases} \phi_n = P^n - \dfrac{n-1}{1}P^{n-2}Q + \dfrac{(n-2)(n-3)}{1\,.\,2}P^{n-4}Q^2 \\ \qquad\qquad - \dfrac{(n-3)(n-4)(n-5)}{1\,.\,2\,.\,3}P^{n-6}Q^3 + \ldots\ , \end{cases}$$

et, en même temps

$$(71)\quad \begin{cases} U_{n+1} = \phi_n U_1 - Q\phi_{n-1}U_0 , \\ V_{n+1} = \phi_n V_1 - Q\phi_{n-1}V_0 , \end{cases}$$

avec les conditions initiales

$$U_0 = 0 , \quad U_1 = 1 , \quad V_0 = 2 , \quad V_1 = P ;$$

par conséquent, on a encore

$$\phi_n = U_{n+1} .$$

On a, en particulier, dans la série de FIBONACCI, pour $P = 1$ et $Q = -1$,

$$(72)\qquad 1 + C_{n-1,1} + C_{n-2,2} + C_{n-3,3} + \ . \ . \ . = u_n ,$$

et, pour $P = 1$, $Q = 1$,

$$(73)\qquad 1 - C_{n-1,1} + C_{n-2,2} - C_{n-3,3} + \ . \ . \ . = \frac{2}{\sqrt{3}}\sin\frac{n\pi}{3}$$

Les formules précédentes se généralisent aisément par la considération de l'équation (8). En effet, si l'on pose

$$(74)\quad \begin{cases} \psi_n = V_r^n - \dfrac{n-1}{1}V_r^{n-2}Q^r + \dfrac{(n-2)(n-3)}{1.2}V_r^{n-4}Q^{2r} \\ \qquad\qquad - \dfrac{(n-3)(n-4)(n-5)}{1.2.3}V_r^{n-6}Q^{3r} + \ . \ . \ . \ . \end{cases}$$

on obtient, comme ci-dessus,

$$(75)\qquad \begin{aligned} U_{m+2nr} &= \psi_{n-1}U_{m+r} - Q^r\psi_{n-2}U_m , \\ V_{m+2nr} &= \psi_{n-1}V_{m+r} - Q^r\psi_{n-2}V_m , \end{aligned}$$

et, pour $m = 0$, on a encore la relation

$$(76)\qquad \psi_{n-1} = \frac{U_{2nr}}{U_r} ,$$

qui permet de calculer inversement la fonction ψ à l'aide des valeurs de U. D'ailleurs, cette relation, dans laquelle n désigne un nombre entier, a lieu quelle que soit la valeur de r ; on a ainsi, pour $r = 0$, la formule

$$(77)\qquad n = 2^{n-1} - C_{n-2,1}2^{n-3} + C_{n-3,2}2^{n-5} - C_{n-4,3}2^{n-7} + \ . \ . \ . \ .$$

Nous ferons observer que les résultats précédents correspondent aux développements bien connus de $\dfrac{\sin nz}{\sin z}$ et de $\cos nz$ suivant les puissances de $\cos z$, obtenus pour la première fois par VIETE.*

* OPERA, Leyde, 1646, pag. 295-299.

SECTION XIII.

De la loi de la répétition des nombres premiers dans les séries récurentes simplement périodiques.

Nous exprimerons encore les fonctions U_{np} et U_{np}, en fonctions entières de U_n et de V_n, par des formules analogues à celles qui ont été données par MOIVRE et par LAGRANGE.*

En effet, si l'on désigne par C_m^n le nombre des combinaisons de m objets pris n à n, on a la relation suivante :

$$(78)\qquad \alpha^p+\beta^p=(\alpha+\beta)^p-\frac{p}{1}\alpha\beta(\alpha+\beta)^{p-2}+\frac{p}{2}C^1_{p-3}\alpha^2\beta^2(\alpha+\beta)^{p-4}+\ldots.$$
$$+(-1)^r\frac{p}{r}C^{r-1}_{p-r-1}\alpha^r\beta^r(\alpha+\beta)^{p-2r}+\ldots.\ ,$$

que l'on peut vérifier *à posteriori*, et dans laquelle tous les coefficients sont entiers, puisque l'on a

$$\frac{p}{r}C^{r-1}_{p-r-1}=C^r_{p-r-1}+C^{r-1}_{p-r-1}.$$

Posons, dans l'hypothèse de p *impair*,

$$\alpha=a^n \quad et \quad \beta=-b^n,$$

nous obtenons

$$(79)\qquad U_{np}=\delta^{p-1}U_n^p+\frac{p}{1}Q^n\delta^{p-3}U_n^{p-2}+\frac{p}{2}C^1_{p-3}Q^{2n}\delta^{p-5}U_n^{p-4}+\ldots.$$
$$+\frac{p}{r}C^{r-1}_{p-r-1}Q^{nr}\delta^{p-2r-1}U_n^{p-2r}+\ldots..$$

La formule précédente conduit à la loi de la répétition des nombres pre²miers dans les séries récurrentes que nous considérons ici. Dans la série naturelle des nombres entiers, un nombre premier p apparait pour la première fois, à son rang, et à la première puissance ; il arrive à la seconde puissance au rang p^2, à la troisième au rang p^3, et ainsi de suite ; de plus, tous les termes divisibles par p^α occupent un rang égal à un multiple quelconque de p^α. Mais dans les séries récurrentes simplement périodiques, il n'en est pas complètement ainsi. Nous démontrons plus loin que les termes de celles-ci contiennent, à des rangs déterminés, tous les nombres premiers ; mais si ces nombres premiers p n'apparaissent pas, pour la première fois, dans la série au rang p, cependant ils s'y reproduisent à intervalles égaux à p, comme dans

* Commentarii Acad. Petrop., t. XIII, ad annum MDCCXLI-XLIII, pag. 29. Leçons sur le calcul des fonctions, pag. 119.

la série ordinaire, et l'apparition de leurs puissances successives se fait comme dans la série naturelle. Ainsi, en général, dans l'étude arithmétique des séries, deux lois sont à considérer : la *loi de l'apparition* des nombres premiers, et la *loi de la répétition.*

Nous démontrerons, pour l'instant, que la loi de la répétition est identiquement la même dans la série naturelle, et dans les séries des U_n. En effet, si p désigne un nombre premier, et U_n le premier terme de la série divisible par p^λ, on observera que le dernier terme de la formule précédente est divisible par $p^{\lambda+1}$, et non par une puissance supérieure de p ; on a donc la proposition fondamentale suivante :

THEOREME : *Si λ désigne le plus grand exposant d'un nombre premier p contenu dans U_n, l'exposant de la plus haute puissance de p, qui divise U_n, est égal à $\lambda+1$.*

Ainsi, par exemple, dans la série de FIBONACCI, u_8 est divisible par 7 ; donc u_{56} est divisible par 7^2 et non par 7^3 ; dans la série de PELL, u_7 et u_{30}, sont respectivement divisibles par 13^2 et par 31^2 ; donc U_{91} et U_{930} sont divisibles par 13^3 et par 31^3, et non par des puissances supérieures.

Inversement, si $a^p \pm b^p$ est divisible par p^λ, $a \pm b$ est divisible par $p^{\lambda-1}$; ce résultat donne des conséquences importantes dans la théorie de l'équation indéterminée

$$x^p + y^p + z^p = 0 ,$$

dont l'irrésolubilité, non démontrée jusqu'à présent, constitue la dernière proposition de FERMAT.

SECTION XIV.

Nouvelles formes linéaires et quadratiques des diviseurs de U_n et de V_n.

La formule (79) donne, successivement, pour p égal à 3, 5, 7, 9, . . . les formules suivantes

$$(80)\quad \begin{cases} U_{3n} = \Delta U_n^3 + 3Q^n U_n , \\ U_{5n} = \Delta^2 U_n^5 + 5Q^n \Delta U_n^3 + 5Q^{2n} U_n , \\ U_{7n} = \Delta^3 U_n^7 + 7Q^n \Delta^2 U_n^5 + 14Q^{2n} \Delta U_n^3 + 7Q^n U_n , \\ U_{9n} = \Delta^4 U_n^9 + 9Q^n \Delta^3 U_n^7 + 27Q^{2n} \Delta^2 U_n^5 + 30Q^{3n} \Delta U_n^3 + 9Q^{4n} U_n , \\ U_{11n} = \Delta^5 U_n^{11} + 11Q^n \Delta^4 U_n^9 + 44Q^{2n} \Delta^3 U_n^7 + 77Q^{3n} \Delta^2 U_n^5 + 55Q^{4n} \Delta U_n^3 + 11Q^{5n} U_n , \\ \text{. . . . . .} \end{cases}$$

On a ainsi

$$\frac{U_{3n}}{U_n} = \Delta U_n^2 + 3Q^n, \tag{81}$$

et, par suite, la proposition suivante :

THEOREME : *Les diviseurs de* $\frac{U_{3n}}{U_n}$ *sont des diviseurs de la forme quadratique* $\Delta x^2 + 3Q^n y^2$.

En particulier, les formes linéaires des diviseurs premiers impairs de $\frac{U_{6n}}{U_{2n}}$ sont

pour la série de FIBONACCI : $30q + 1, 17, 19, 23$;
" " FERMAT : $6q + 1$;
" " PELL : $24q + 1, 5, 7, 11$;

et les formes linéaires des diviseurs premiers impairs de $\frac{U_{3(2n+1)}}{U_{2n+1}}$ sont

pour la série de FIBONACCI : $60q + 1, 7, 11, 17, 43, 49, 53, 59$;
" " FERMAT : $24q + 1, 5, 7, 11$;
" " PELL : $24q + 1, 5, 19, 23$.

On a aussi

$$4\frac{U_{5n}}{U_n} = (2\Delta U_n^2 + 5Q^n)^2 - 5Q^{2n}, \tag{82}$$

et, par suite :

THEOREME : *Les diviseurs de* $\frac{U_{5n}}{U_n}$ *sont des diviseurs de la forme quadratique* $x^2 - 5y^2$.

Les formes linéaires des diviseurs premiers impairs sont, dans les trois séries prises pour exemples,

$$20q + 1,\ 9,\ 11,\ 19.$$

Nous avons aussi

$$4\frac{U_{7n}}{U_n} = \Delta\left[2\Delta U_n^3 + 7Q^n U_n\right]^2 + 7Q^{2n}V_n^2, \tag{83}$$

et, par suite :

THEOREME : *Les diviseurs de* $\frac{U_{7n}}{U_n}$ *sont des diviseurs de la forme quadratique* $\Delta x^2 + 7y^2$.

Supposons maintenant que p désigne un nombre *pair*, et faisons encore, dans la formule (78),

$$\alpha = a^n, \quad \beta = -b^n,$$

nous obtenons

$$V_{np} = \delta^p U_n^p + \frac{p}{1} Q^n \delta^{p-2} U_n^{p-2} + \frac{p}{2} C_{p-3}^1 Q^{2n} \delta^{p-4} U^{p-4} + \ldots . \tag{84}$$
$$+ \frac{p}{r} C_{p-r-1}^{r-1} Q^{nr} \delta^{p-2r} U_n^{p-2r} + \ldots .$$

On a, en particulier, pour $p = 2$, la formule

$$V_{2n} = \Delta U_n^2 + 2Q^n , \tag{85}$$

et, par conséquent, la proposition suivante :

Théorème : *Les diviseurs de* V_{2n} *sont des diviseurs de la forme quadratique* $\Delta x^2 + 2Q^n y^2$.

Les formes linéaires correspondantes des diviseurs premiers impairs sont, pour *n pair*

dans la série de FIBONACCI : $40q + 1, 7, 9, 11, 13, 19, 23, 37$;
" " FERMAT : $8q + 1, 3$;
" " PELL : $4q + 1$;

et, pour *n impair*

dans la série de FIBONACCI : $40q + 1, 3, 9, 13, 27, 31, 37, 39$;
" " FERMAT : $4q + 1$;
" " PELL : $4q + 1$;

On devra, dans les applications, combiner ces résultats avec ceux que nous avons donnés dans la Section VIII.

Faisons enfin dans la formule (79),

$$\alpha = a^n , \quad \beta = b^n ,$$

nous obtenons, en supposant indifféremment que p est égal à un nombre *pair* ou à un nombre *impair* :

$$V_{np} = V_n^p - \frac{p}{1} Q^n V_n^{p-2} + \frac{p}{2} C_{p-3}^1 Q^{2n} V_n^{p-4} - \ldots + (-1)^r \frac{p}{r} C_{p-r-1}^{r-1} Q^{nr} V_n^{p-2r} + \ldots \tag{86}$$

On a ainsi, en faisant successivement p égal à 2, 3, 4, 5, 6, . . . les résultats suivants

$$\left\{ \begin{array}{l} V_{2n} = V_n^2 - 2Q^n , \\ V_{3n} = V_n^3 - 3Q^n V_n , \\ V_{4n} = V_n^4 - 4Q^n V_n^2 + 2Q^{2n} , \\ V_{5n} = V_n^5 - 5Q^n V_n^3 + 5Q^{2n} V_n , \\ V_{6n} = V_n^6 - 6Q^n V_n^4 + 9Q^{2n} V_n^2 - 2Q^{3n} , \\ \ldots \ldots \ldots \ldots \ldots \ldots \end{array} \right. \tag{87}$$

qui conduisent encore à des formules entièrement semblables aux précédentes.

SECTION XV.

Des relations des.fonctions U_n et V_n avec les radicaux continus.

On tire de l'équation

$$x^2 = Px - Q ,$$

la formule

$$x = \sqrt{-Q + Px} ,$$

et, successivement

$$x = \sqrt{-Q + P\sqrt{-Q + Px}} ,$$

$$x = \sqrt{-Q + P\sqrt{-Q + P\sqrt{-Q + Px}}} ,$$

. . . . . ;

par conséquent, puisque l'on peut supposer P positif, on a, pour Q négatif,

$$a = \text{Lim.}\sqrt{-Q + P\sqrt{-Q + P\sqrt{-Q + \ldots.}}} , \tag{88}$$

a désignant la racine positive de l'équation proposée. Ainsi, dans la série de FIBONACCI

$$\frac{1+\sqrt{5}}{2} = \text{Lim.}\sqrt{1 + \sqrt{1 + \sqrt{1 + \sqrt{1 + \ldots.}}}} ,$$

dans, la série de PELL,

$$1 + \sqrt{2} = \text{Lim.}\sqrt{1 + 2\sqrt{1 + 2\sqrt{1 + 2\sqrt{1 + \ldots.}}}} ,$$

et, dans la série de FERMAT,

$$2 = \text{Lim.}\sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{2 + \ldots.}}}} .$$

On sait que ce dernier radical se présente dans le calcul de π, par la méthode des périmètres, imaginée par ARCHIMEDE.

Mais les résultats obtenus dans la section précédente, conduisent à des formules plus importantes, qui trouveront leur emploi dans la recherche des grands nombres premiers. On tire, par exemple, de la première des formules (87)

$$V_n = \sqrt{2Q^n + V_{2n}} ;$$

et, de même, en changeant n en $2n$, $4n$, $8n$, ...

$$V_{2n} = \sqrt{2Q^{2n} + V_{4n}} ,$$

$$V_{4n} = \sqrt{2Q^{4n} + V_{8n}} ,$$

$$V_{8n} = \sqrt{2Q^{8n} + V_{16n}} ;$$

et, par suite,

$$(89)\quad \begin{cases} V_n = \sqrt{2Q^n + V_{2n}}\,, \\ V_n = \sqrt{2Q^n + \sqrt{2Q^{2n} + V_{4n}}}\,, \\ V_n = \sqrt{2Q^n + \sqrt{2Q^{2n} + \sqrt{2Q^{4n} + V_{8n}}}}\,, \\ V_n = \sqrt{2Q^n + \sqrt{2Q^{2n} + \sqrt{2Q^{4n} + \sqrt{2Q^{8n} + V_{16n}}}}}\,, \\ \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad , \end{cases}$$

et ainsi indéfiniment. Ces formules sont analogues à celles que l'on obtient pour $\cos\frac{\pi}{4}$, $\cos\frac{\pi}{8}$, $\cos\frac{\pi}{16}$, $\cos\frac{\pi}{32}$, . . . $\cos\frac{\pi}{2^r}$.

La seconde des relations (87) donne de la même façon

$$(90)\quad \begin{cases} V_n = \sqrt{3Q^n + \frac{V_{3n}}{V_n}}\,, \\ V_n = \sqrt{2Q^n + \sqrt{3Q^{2n} + \frac{V_{6n}}{V_{2n}}}}\,, \\ V_n = \sqrt{2Q^n + \sqrt{2Q^{2n} + \sqrt{3Q^{4n} + \frac{V_{12n}}{V_{4n}}}}}\,, \end{cases}$$

ces formules sont semblables à celles que l'on obtient pour $\cos\frac{\pi}{6}$, $\cos\frac{\pi}{12}$, $\cos\frac{\pi}{24}$, . . . $\cos\frac{\pi}{3.2^r}$.

La troisième des relations (87) conduit encore à des formules qui correspondent à celles qui donnent $\cos\frac{\pi}{10}$, $\cos\frac{\pi}{20}$, $\cos\frac{\pi}{40}$, . . . $\cos\frac{\pi}{5.2^r}$; et ainsi de quelques autres.

SECTION XVI.

Dévelopements des puissances de U_n et de V_n en fonctions linéaires des termes dont les arguments sont des multiples de n.

On peut exprimer les puissances de *Un* et de *Vn* en fonctions linéaires des termes dont les rangs sont des multiples de *n*, par des formules analogues à celles qui donnent les puissances de sin *z* et de cos *z*, développées suivant les sinus,et les cosinus des multiples de l'arc *z*. En désignant d'abord par *p* un nombre *impair*, le développement de $(\alpha - \beta)^p$, donne

$$(\alpha-\beta)^p = (\alpha^p - \beta^p) - \frac{p}{1}\alpha\beta(\alpha^{p-2} - \beta^{p-2}) + \frac{p(p-1)}{1\,.\,2}\alpha^2\beta^2(\alpha^{p-4} - \beta^{p-4}) - \ldots$$

et, par suite, en faisant

$$\alpha = a^n, \quad \beta = b^n,$$

on obtient la formule

$$(91)\qquad \Delta^{\frac{p-1}{2}} U_n^p = U_{pn} - \frac{p}{1} Q^n U_{(p-2)n} + \frac{p(p-1)}{1.2} Q^{2n} U_{(p-4)n}$$

$$- \frac{p(p-1)(p-2)p}{1.2.3} Q^{3n} U_{(p-6)n} + \ldots + \ldots \pm \frac{p(p-1)\ldots\frac{p+3}{2}}{1.2\ldots.\frac{p-1}{2}} Q^{\frac{p-1}{2}} U_n \ .$$

On a successivement, pour p égal à 3, 5, 7, 9, ...

$$(92)\qquad \begin{cases} \Delta U_n^3 = U_{3n} - 3Q^n U_n, \\ \Delta^2 U_n^5 = U_{5n} - 5Q^n U_{3n} + 10Q^{2n} U_n, \\ \Delta^3 U_n^7 = U_{7n} - 7Q^n U_{5n} + 21Q^{2n} U_{3n} - 35Q^{4n} U_n, \\ \Delta^4 U_n^9 = U_{9n} - 9Q^n U_{7n} + 36Q^{2n} U_{5n} - 84Q^{4n} U_{3n} + 126Q^{6n} U_n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Le développement de $(\alpha - \beta)^p$ donne encore, en supposant maintenant que p désigne un nombre *pair* :

$$(93)\qquad \Delta^{\frac{p}{2}} U_n^p = V_{pn} - \frac{p}{1} Q^n V_{(p-2)n} + \frac{p(p-1)}{1.2} Q^{2n} V_{(p-4)n}$$

$$- \frac{p(p-1)(p-2)p}{1.2.3} Q^{3n} V_{(p-6)n} + \ldots + \ldots \pm \frac{p(p-1)\ldots\frac{p}{2}+1}{1.2\ldots.\frac{p}{2}} Q^{\frac{p}{2}n},$$

et, pour p successivement égal à 2, 4, 6, 8, . . .

$$(94)\qquad \begin{cases} \Delta U_n^2 = V_{2n} - 2Q^n, \\ \Delta^2 U_n^4 = V_{4n} - 4Q^n V_{2n} + 6Q^{2n}, \\ \Delta^3 U_n^6 = V_{6n} - 6Q^n V_{4n} + 15Q^{2n} V_{2n} - 20Q^{3n}, \\ \Delta^4 U_n^8 = V_{8n} - 8Q^n V_{6n} + 28Q^{2n} V_{4n} - 56Q^{3n} V_{2n} + 70Q^{4n}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Le développement de $(\alpha - \beta)^p$ donne, dans l'hypothèse de p égal à un nombre *impair*,

$$(95)\qquad V_n^p = V_{np} + \frac{p}{1} Q^n V_{(p-2)n} + \frac{p(p-1)}{1.2} Q^{2n} V_{(p-4)n}$$

$$+ \frac{p(p-1)(p-2)}{1.2.3} Q^{3n} V_{(p-6)n} + \ldots + \ldots + \frac{p(p-1)\ldots\frac{p+3}{2}}{1.2\ldots\frac{p-1}{2}} Q^{\frac{p-1}{2}n} V_n \ ,$$

et, plus particulièrement

$$(96)\quad \begin{cases} V_n^3 = V_{3n} + 3Q^n V_n, \\ V_n^5 = V_{5n} + 5Q^n V_{3n} + 10Q^{2n} V_n, \\ V_n^7 = V_{7n} + 7Q^n V_{5n} + 21Q^{2n} V_{3n} + 35Q^{3n} V_n, \\ V_n^9 = V_{9n} + 9Q^n V_{7n} + 36Q^{2n} V_{5n} + 84Q^{3n} V_{3n} + 126Q^{4n} V_n, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{cases}$$

De même, lorsque p désigne un nombre *pair*,

$$(97)\quad V_n^p = V_{np} + \frac{p}{1} Q^n V_{(p-2)n} + \frac{p(p-1)}{1.2} Q^{2n} V_{(p-4)n}$$

$$+ \frac{p(p-1)(p-2)}{1.2.3} Q^{3n} V_{(p-6)n} + \ldots + \ldots + \frac{p(p-1)\ldots\left(\frac{p}{2}+1\right)}{1.2\ldots\left(\frac{p}{2}\right)} Q^{\frac{p}{2}n},$$

on a, plus particulièrement,

$$(98)\quad \begin{cases} V_n^2 = V_{2n} + 2Q^n, \\ V_n^4 = V_{4n} + 4Q^n V_{2n} + 6Q^{2n}, \\ V_n^6 = V_{6n} + 6Q^n V_{4n} + 15Q^{2n} V_{2n} + 20Q^{3n}, \\ V_n^8 = V_{8n} + 8Q^n V_{6n} + 28Q^{2n} V_{4n} + 56Q^{3n} V_{2n} + 70Q^{4n}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{cases}$$

Les relations (91), (93), (95) et (97) sont elles mêmes des cas particuliers des formules suivantes :

$$(99)\quad \begin{cases} V_r^n U_{(m-n)r} = U_{mr} + \frac{n}{1} Q^r U_{(m-2)r} + \frac{n(n-1)}{1.2} Q^{2r} U_{(m-4)r} + \frac{n(n-1)(n-2)}{1.2.3} Q^{3r} U_{(m-6)r} + \ldots, \\ V_r^n V_{(m-n)r} = V_{mr} + \frac{n}{1} Q^r V_{(m-2)r} + \frac{n(n-1)}{1.2} Q^{2r} V_{(m-4)r} + \frac{n(n-1)(n-2)}{1.2.3} Q^{3r} V_{(m-6)r} + \ldots, \\ \Delta^n U_r^{2n} U_{(m-2n)r} = U_{mr} - \frac{2n}{1} Q^r U_{(m-2)r} + \frac{2n(n-1)}{1.2} Q^{2r} U_{(m-4)r} - \ldots, \\ \Delta^n U_r^{2n} V_{(m-2n)r} = V_{mr} - \frac{2n}{1} Q^r V_{(m-2)r} + \frac{2n(2n-1)}{1.2} Q^{2r} V_{(m-4)r} - \ldots, \\ \Delta^n U_r^{2n+1} U_{(m-2n-1)r} = U_{mr} - \frac{2n+1}{1} Q^r U_{(m-2r)} + \frac{(2n+1).2n}{1.2} Q^{2r} U_{(m-4)r} - \ldots, \\ \Delta^n U_r^{2n+1} V_{(m-2n-1)r} = V_{mr} - \frac{2n+1}{1} Q^r V_{(m-2r)} + \frac{(2n+1).2n}{1.2} Q^{2r} V_{(m-4)r} - \ldots \end{cases}$$

Ces relations trouvent principalement leur emploi dans la sommation des puissances semblables des fonctions U_n et V_n. Le développement de la puissance d'un binôme donne encore lieu à un certain nombre d'autres. Ainsi, on a, par exemple

$$\alpha = \overline{\alpha+\beta} - \beta \quad \text{et} \quad \beta = \overline{\beta+\alpha} - \alpha \ ;$$

donc, pour p égal à un nombre *impair*

$$\alpha^p + \beta^p = (\alpha+\beta)^p - \frac{p}{1}\beta(\alpha+\beta)^{p-1} + \frac{p(p-1)}{1.2}\beta^2(\alpha+\beta)^{p-2} + \ldots + \frac{p}{1}\beta^{p-1}(\alpha+\beta),$$

$$\alpha^p + \beta^p = (\alpha+\beta)^p - \frac{p}{1}\alpha(\alpha+\beta)^{p-1} + \frac{p(p-1)}{1.2}\alpha^2(\alpha+\beta)^{p-2} + \ldots + \frac{p}{1}\alpha^{p-1}(\alpha+\beta),$$

on a ainsi, en ajoutant et en retranchant, après avoir posé $\alpha = a^n$, $\beta = b^n$, les formules suivantes :

$$(100)\quad \begin{cases} 2V_{np} = V_0 V_n^p - \dfrac{p}{1}V_n V_n^{p-1} + \dfrac{p(p-1)}{1.2}V_{2n}V_n^{p-2} + \ldots + \dfrac{p}{2}V_{(p-1)n}V_n, \\ 0 = \dfrac{p}{1}U_n V_n^{p-1} - \dfrac{p(p-1)}{1.2}U_{2n}V_n^{p-2} + \ldots - \dfrac{p}{1}U_{(p-1)n}V_n. \end{cases}$$

On trouvera des développements analogues pour p égal à un nombre pair, et d'autres encore à l'aide des identités

$$\alpha = \overline{\alpha-\beta} + \beta \quad \text{et} \quad \beta = \overline{\beta-\alpha} + \alpha \ ;$$

La formule suivante, que l'on peut déduire du *Problème des partis*

$$(\alpha+\beta)^{p+q-1} = \alpha^p\left[(\alpha+\beta)^{q-1} + \frac{p}{1}(\alpha+\beta)^{q-2}\beta + \frac{p(p+1)}{1.2}(\alpha+\beta)^{q-3}\beta^2 + \ldots + C_{p+q-2}^{q-1}\beta^{q-1}\right]$$
$$+ \beta^q\left[(\alpha+\beta)^{p-1} + \frac{q}{1}(\alpha+\beta)^{p-2}\alpha + \frac{q(q+1)}{1.2}(\alpha+\beta)^{q-3}\alpha^2 + \ldots + C_{p+q-2}^{p-1}\alpha^{q-1}\right],$$

donne en changeant α en β puis par addition et par soustraction,

$$(101)\quad \begin{cases} 2V_n^{p+q-1} = V_{pn}V_n^{q-1} + \dfrac{p}{1}Q^n V_{(p-1)n}V_n^{q-2} + \dfrac{p(p+1)}{1.2}Q^{2n}V_{(p-2)n}V_n^{q-3} \\ \quad + \ldots + C_{p+q-2}^{q-1}Q^{(q-1)n}V_{(p-q+1)n} + V_{qn}V_n^{p-1} + \dfrac{q}{1}Q^n V_{(q-1)n}V_n^{p-2} \\ \quad + \dfrac{q(q+1)}{1.2}Q^{2n}V_{(q-2)n}V_n^{p-3} + \ldots + C_{p+q-2}^{p-1}Q^{(p-1)}V^{(q-p+1)n}, \\ 0 = U_{pn}V_n^{q-1} + \dfrac{p}{1}Q^n U_{(p-1)n}V_n^{q-2} + \dfrac{p(p+1)}{1.2}Q^{2n}U_{(p-2)n}V_n^{q-3} \\ \quad + \ldots + C_{p+q-2}^{q-1}Q^{(q-1)n}U_{(p-q+1)n} - U_{qn}V_n^{p-1} - \dfrac{q}{1}Q^n U_{(q-1)n}V_n^{p-2} \\ \quad - \dfrac{q(q+1)}{1.2}Q^{2n}U_{(q-2)n}V_n^{p-3} - \ldots - C_{p+q-2}^{p-1}Q^{(p-1)}U_{(q-p+1)n}. \end{cases}$$

On obtiendrait deux autres formules semblables aux précédentes, en po-

sant $\alpha = a^n$, $\beta = b^n$; on simplifie ces formules, en faisant $p = q$.

SECTION XVII.

Autres formules concernant le développement des fontions numériques U_n et V_n.

Considérons les fonctions α et β de z,

$$\alpha = \left(\frac{z + \sqrt{z^2 - 4h}}{2} \right)^n , \qquad \beta = \left(\frac{z - \sqrt{z^2 - 4h}}{2} \right)^n ;$$

on tire, en différentiant $\dfrac{d\alpha}{\alpha dz} = \dfrac{n}{\sqrt{z^2 - 4h}}$,

et, en faisant disparaitre le radical

$$(z^2 - 4h)\frac{d\alpha^2}{dz^2} - n^2\alpha^2 = 0 .$$

Une nouvelle différentiation nous donne

$$(z^2 - 4h)\frac{d^2\alpha}{dz^2} + z\frac{d\alpha}{dz} - n^2\alpha^2 = 0 .$$

il est d'ailleurs facile de voir que les fonctions β, $\alpha + \beta$ et $\alpha - \beta$ vérifient la même équation différentielle. On a donc, en désignant par $f(z)$ l'une quelconque d'entre elles, par l'application du théorème de LEIBNIZ

$$(z^2 - 4h)\frac{d^{p+2} f(z)}{dz^{p+2}} + (2p+1)z\frac{d^{p+1} f(z)}{dz^{p+1}} + (p^2 - n^2)\frac{d^p f(z)}{dz^p} = 0 ,$$

et, pour $z = 0$, $\qquad 4h\dfrac{d^{p+2} f(0)}{dz^{p+2}} = (p^2 - n^2)\dfrac{d^p f(0)}{dz^p}$.

Si l'on suppose $z = V_r$, $h = Q^r$, la formule de MACLAURIN nous donne, pour *n pair*, les deux développements

$$(102)\quad \begin{cases} \dfrac{V_{nr}}{2(-Q^r)^{\frac{n}{2}}} = 1 - \dfrac{n^2}{1.2}\dfrac{V_r^2}{2^2 Q^r} + \dfrac{n^2(n^2-2^2)}{1.2.3.4}\dfrac{V_r^4}{2^4 Q^{2r}} - \dfrac{n^2(n^2-2^2)(n^2-4^2)}{1.2.3.4.5.6}\dfrac{V_r^6}{2^6 Q^{3r}} + \ldots , \\ \dfrac{-U_{nr}}{2(-Q^r)^{\frac{n}{2}} U_r} = \dfrac{n}{1}\dfrac{V_r}{2Q^r} - \dfrac{n(n^2-2^2)}{1.2.3}\dfrac{V_r^3}{2^3 Q^{3r}} + \dfrac{n(n^2-2^2)(n^2-4^2)}{1.2.3.4.5}\dfrac{V_r^5}{2^5 Q^{5r}} - \ldots \end{cases}$$

et, pour *n impair*,

$$(103)\quad \begin{cases} \dfrac{U_{nr}}{(-Q^r)^{\frac{n-1}{2}}} = U_r\left[1 - \dfrac{n^2-1^2}{1.2}\dfrac{V_r^2}{2^2 Q^r} + \dfrac{(n^2-1^2)(n^2-3^2)}{1.2.3.4}\dfrac{V_r^4}{2^4 Q^{2r}} - \ldots \right], \\ \dfrac{-V_{nr}}{2(-Q^r)^{\frac{n-1}{2}}} = V_r\left[n - \dfrac{n(n^2-1^2)}{1.2.3}\dfrac{V_r^2}{2^2 Q^r} + \dfrac{n(n^2-1^2)(n^2-3^2)}{1.2.3.4.5}\dfrac{V_r^4}{2^4 Q^{2r}} - \ldots \right]. \end{cases}$$

On peut d'ailleurs vérifier ces formules, et les suivantes, *à posteriori*, en observant que si l'on pose

$$G_{m,x} = (m^2 - 2^2)(m^2 - 4^2) \ldots (m^2 - 4x^2) ,$$
$$H_{m,x} = (m^2 - 1^2)(m^2 - 3^2) \ldots (m^2 - (2x-1)^2) ,$$

on a les relations

$$mG_{m,x} = (m - 2x)H_{m+1,x} = (m + 2x)H_{m-1,x} .$$

Au lieu de développer les fonctions U_{nr} et V_{nr} suivant les puissances de V_r, on peut aussi les développer suivant les puissances de U_r ; on trouve ainsi, pour *n pair*

$$(104)\quad \begin{cases} \dfrac{V_{nr}}{2Q^{\frac{nr}{2}}} = 1 + \dfrac{n^2}{1.2}\dfrac{\Delta U_r^2}{2^2 Q^r} + \dfrac{n^2(n^2-2^2)}{1.2.3.4}\dfrac{\Delta^2 U_r^4}{2^4 Q^{2r}} + \dfrac{n^2(n^2-2^2)(n^2-4^2)}{1.2.3.4.5}\dfrac{\Delta^3 U_r^6}{2^6 Q^{3r}} + \ldots , \\ \dfrac{U_{nr}}{Q^{\left(\frac{n}{2}-1\right)r}} = \dfrac{U_{2r}}{2}\left[n + \dfrac{n(n^2-2^2)}{1.2.3}\dfrac{\Delta U_r^2}{2^2 Q^r} + \dfrac{n(n^2-2^2)(n^2-4^2)}{1.2.3.4.5}\dfrac{\Delta^2 U_r^4}{2^4 Q^{2r}} - \ldots \right], \end{cases}$$

et, pour *n impair*

$$(105)\quad \begin{cases} \dfrac{V_{nr}}{2Q^{\frac{n-1}{2}r}} = V_r\left[1 + \dfrac{n^2-1^2}{1.2}\dfrac{\Delta U_r^2}{2^2 Q^r} + \dfrac{(n^2-1^2)(n^2-3^2)}{1.2.3.4}\dfrac{\Delta^2 U_r^4}{2^4 Q^{2r}} + \right. \\ \qquad\qquad \left. \dfrac{(n^2-1^2)(n^2-3^2)(n^2-5^2)}{1.2.3.4.5.6}\dfrac{\Delta^3 U_r^6}{2^6 Q^{3r}} + \ldots \right], \\ \dfrac{U_{nr}}{Q^{\frac{n-1}{2}r}} = U_r\left[n + \dfrac{n(n^2-1^2)}{1.2.3}\dfrac{\Delta U_r^2}{2^2 Q^r} + \dfrac{n(n^2-1^2)(n^2-3^2)}{1.2.3.4.5}\dfrac{\Delta^2 U_r^4}{2^4 Q^{2r}} \right. \\ \qquad\qquad \left. + \dfrac{n(n^2-1^2)(n^2-3^2)(n^2-5^2)}{1.2.3.4.5.6.7}\dfrac{\Delta^3 U_r^6}{2^6 Q^{3r}} + \ldots , \right]. \end{cases}$$

En ayant égard à l'une ou l'autre des relations

$$V_{nr}^2 = V_{2nr} + 2Q^{nr} , \quad \text{et} \quad \Delta U_{nr}^2 = V_{2nr} - 2Q^{nr} ,$$

on obtiendra de nouvelles formules, et ainsi, par exemple :

$$(106)\qquad \frac{U_{nr}^2}{Q^{(n-2)r}U_r} = n^2 - \frac{n^2(n^2-1^2)}{3.4}\frac{\Delta U_r^2}{Q^r} + \frac{n^2(n^2-1^2)(n^2-2^2)}{3.4.5.6}\frac{\Delta^2 U_r^4}{Q^{2r}} - \ldots$$

On peut d'ailleurs mettre cette dernière formule et quelques autres sous une forme assez remarquable, en observant que l'on a, pour m quelconque et n entier positif, l'identité

$$\frac{m^2(m^2-1^2)(m^2-3^2)\ldots(m^2-(n-1)^2)}{3.4.5.\ldots\ldots(2n)} = \frac{(m-n)(m-n+1)(m-n+2)\ldots(m+n-1)}{3.4.5.\ldots\ldots(2n)} + \frac{(m-n+1)(m-n+2)\ldots(m+n)}{3.4.5.\ldots\ldots(2n)} .$$

Par conséquent, les coefficients de la formule (106) sont entiers, et l'on a

$$\frac{n^2(n^2-1^2)(n^2-2^2)\ldots(n^2-\overline{r-1}^2)}{3\,.\,4\,.\,5\,.\ldots\ldots\,.(2r)} = C_{n+r-1}^{2r} + C_{n+r}^{2r}\ .\ ^{*}$$

Nous ferons observer que les formules (104) et (105) subsistent encore pour des valeurs quelconques de n ; on a alors des développements en séries convergentes, lorsque $\frac{\Delta U_r^2}{2^2 Q^r}$ n'est pas supérieur à l'unité ; en effet, si l'on pose

$$\frac{\Delta U_r^2}{2^2 Q^r} \leq 1,$$

le rapport d'un terme au précédent finit par devenir négatif (pour Δ positif), et inférieur à l'unité en valeur absolue. Cette condition est remplie pour $r = 1$ dans la série de PELL ; on a donc, quelle que soit la valeur de n

$$(107)\quad \begin{cases} \frac{1}{2}\left[\left(\sqrt{2}+1\right)^n + \left(\sqrt{2}-1\right)^n\right] = 1 + \frac{n^2}{1\,.\,2} + \frac{n^2(n^2-2^2)}{1\,.\,2\,.\,3\,.\,4} + \\ \qquad\qquad \frac{n^2(n^2-2^2)(n^2-4^2)}{1\,.\,2\,.\,3\,.\,4\,.\,5\,.\,6} + \ldots\ , \\ \frac{1}{2}\left[\left(\sqrt{2}+1\right)^n + \left(\sqrt{2}-1\right)^n\right] = n + \frac{n(n^2-1^2)}{1\,.\,2\,.\,3} + \frac{n(n^2-1^2)(n^2-3^2)}{1\,.\,2\,.\,3\,.\,4\,.\,5} + \ldots\ . \end{cases}$$

SECTION XVIII.

Développements en séries des irrationnelles et de leurs logarithmes népériens.

Les développements des fonctions en séries, par la formule de MACLAURIN, donnent lieu à un très-grand nombre de formules nouvelles, pour le développement des fonctions numériques que nous considérons ici, et par suite, pour celui des fonctions circulaires et hyperboliques. Lorsque les séries correspondantes ne sont convergentes que pour les valeurs de la variable dont le module est inférieur à une limite donnée, on peut toujours supposer que cette variable x est choisie de telle sorte que la série représente la fonction, pour toutes les valeurs de x dont le module est inférieur à l'unité. Soit donc la série

$$F(x) = A_0 + A_1 x + A_2 x^2 + A_3 x^3 + A_4 x^4 + \ldots\ ;$$

---

[*] En désignant par a le résidu de n^2 suivant le module p, premier avec n, on déduit de cette identité une démonstration immédiate d'une proposition contenue au No. 128 des *Disqisitiones Arithmeticæ*.

on aura, en supposant z positif,

$$F\left(\frac{z}{1+z}\right)=A_0+A_1\frac{z}{1+z}+A_2\frac{z^2}{(1+z)^2}+A_3\frac{z^3}{(1+z)^3}+\ldots,$$
$$F\left(\frac{1}{1+z}\right)=A_0+A_1\frac{1}{1+z}+A_2\frac{1}{(1+z)^2}+A_3\frac{1}{(1+z)^3}+\ldots,$$

et, par conséquent:

$$F\left(\frac{1}{1+z}\right)+F\left(\frac{z}{1+z}\right)=2A_0+A_1\frac{1+z}{1+z}+A_2\frac{1+z^2}{(1+z)^2}+A_3\frac{1+z^3}{(1+z)^3}+\ldots,$$
$$F\left(\frac{1}{1+z}\right)-F\left(\frac{z}{1+z}\right)=\quad+A_1\frac{1-z}{1+z}+A_2\frac{1-z^2}{(1+z)^2}+A_3\frac{1-z^3}{(1+z)^3}+\ldots.$$

Si l'on désigne par a la plus grande des racines, supposée positive, de l'équation fondamentale (1), par r un nombre *pair*, ou un nombre entier quelconque, suivant que la racine b est négative ou positive, et si l'on pose $z=\frac{b^r}{a^r}$, on obtient

$$(108)\quad\begin{cases} F\left(\frac{a^r}{a^r+b^r}\right)+F\left(\frac{a^rb^r}{a^r+b^r}\right)=2A_0+A_1\frac{V_r}{V_r}+A_2\frac{V_{2r}}{V_r^2}+A_3\frac{V_{3r}}{V_r^3}+\ldots., \\ F\left(\frac{a^r}{a^r+b^r}\right)-F\left(\frac{a^rb^r}{a^r+b^r}\right)=\sqrt{\Delta}\left[A_1\frac{U_r}{V_r}+A_2\frac{U_{2r}}{V_r^2}+A_3\frac{U_{3r}}{V_r^3}+\ldots\right]. \end{cases}$$

Si l'on suppose $z=-\frac{b^r}{a^r}$, on obtient deux développements analogues aux précédents ; ces développements sont parfois, très-lentement convergents ; mais leur étude conduit à des propriétés importantes dans la théorie des nombres premiers.

Le développement du binôme $(1-x)^m$ donne ainsi, pour m quelconque, les séries

$$(109)\quad\begin{cases} \frac{V_{mr}}{V_r^m}=V_0-\frac{m}{1}\frac{V_r}{V_r}+\frac{m(m-1)}{1.2}\frac{V_{2r}}{V_r^2}-\frac{m(m-1)(m-2)}{1.2.3}\frac{V_{3r}}{V_r^3}+\ldots., \\ \frac{U_{mr}}{V_r^m}=\frac{m}{1}\frac{U_r}{V_r}-\frac{m(m-1)}{1.2}\frac{U_{2r}}{V_r^2}-\frac{m(m-1)(m-2)}{1.2.3}\frac{U_{3r}}{V_r^3}+\ldots., \end{cases}$$

que l'on aurait pu déduire de la série de BERNOULLI ; pour $m=-1$, on a

$$(110)\quad\begin{cases} \frac{V_r^2}{Q^r}=V_0+\frac{V_r}{V_r}+\frac{V_{2r}}{V_r^2}+\frac{V_{3r}}{V_r^3}+\ldots., \\ \frac{U_r^2}{Q^r}=\frac{U_r}{V_r}+\frac{U_{2r}}{V_r^2}+\frac{U_{3r}}{V_r^3}+\frac{U_{4r}}{V_r^4}+\ldots., \end{cases}$$

et, par exemple, dans la série de FIBONACCI

$$(111)\quad \begin{cases} 9 = 2 + \dfrac{3}{3} + \dfrac{7}{9} + \dfrac{18}{27} + \dfrac{47}{81} + \ldots., \\ 3 = \dfrac{1}{3} + \dfrac{3}{9} + \dfrac{8}{27} + \dfrac{21}{81} + \dfrac{55}{243} + \ldots.; \end{cases}$$

les numérateurs de ces deux séries de fractions sont donnés par la relation de récurrence

$$N_{n+2} = 3N_{n+1} - N_n.$$

On obtiendra des formules semblables pour $m = \pm\frac{1}{2}$ le développement de

$$(1 + x)^m \pm (1 - x)^m$$

donne des formules analogues aux relations (109).

Le développement de $\operatorname{Log}(1 - x)$ donne les formules

$$(112)\quad \begin{cases} \operatorname{Log}\dfrac{V_r^2}{Q^r} = 1 + \dfrac{1}{2}\dfrac{V_{2r}}{V_r^2} + \dfrac{1}{3}\dfrac{V_{3r}}{V_r^3} + \dfrac{1}{4}\dfrac{V_{4r}}{V_r^4} + \ldots., \\ \operatorname{Log}\dfrac{b^{2r}}{Q^r} = 2\sqrt{\Delta}\left[\dfrac{U_r}{V_r} + \dfrac{1}{2}\dfrac{U_{2r}}{V_r^2} + \dfrac{1}{3}\dfrac{U_{3r}}{V_r^3} + \dfrac{1}{4}\dfrac{U_{4r}}{V_r^4} + \ldots\right]; \end{cases}$$

celui de $\operatorname{Log}\frac{1-x}{1+x}$ donne

$$(113)\qquad \operatorname{Log}\frac{b^{2r}}{Q^r} = 2\sqrt{\Delta}\left[\frac{U_r}{V_r} + \frac{1}{3}\frac{\Delta U_{3r}}{V_r^3} + \frac{1}{5}\frac{\Delta^2 U_{5r}}{V_r^5} + \frac{1}{7}\frac{\Delta^3 U_{7r}}{V_r^7} + \ldots\right],$$

et, dans la série de PELL

$$(114)\qquad \sqrt{2}\operatorname{Log}(1+\sqrt{2}) = 1 + \frac{1}{2.3} + \frac{1}{2^2.5} + \frac{1}{2^3.7} + \frac{1}{2^5.9} + \ldots\ .$$

La formule

$$\frac{1}{2}\operatorname{Log}\frac{z+h}{z-h} = hz\left[\frac{1}{z^2-h^2} - \frac{2}{3}\frac{h^2}{(z^2-h^2)^2} + \frac{2.4}{3.5}\frac{h^4}{(z^2-h^2)^3} - \frac{2.4.6}{3.5.7}\frac{h^6}{(z^2-h^2)^4} + \ldots\right]$$

dans laquelle on suppose

$$z + h = a^r, \qquad z - h = b^r, \qquad z^2 - h^2 = Q^r, \qquad h^2 = \frac{\Delta U_r^2}{4},$$

donne encore

$$(115)\quad \operatorname{Log}\frac{a^{2r}}{Q^r} = \frac{2\sqrt{\Delta}U_r}{2}\left[\frac{1}{Q^r} - \frac{2}{3}\frac{\Delta U_r^2}{2^2 Q^{2r}} + \frac{2.4}{3.5}\frac{\Delta^2 U_r^4}{2^3 Q^{3r}} - \frac{2.4.6}{3.5.7}\frac{\Delta^3 U_r^6}{2^4 Q^{4r}} + \ldots\right];$$

pour que cette série soit convergente, on doit avoir $\Delta U_r^2 \leq 4Q^r$; on trouve ainsi, à la limite de convergence

$$(116)\qquad \operatorname{Log}(1+\sqrt{2}) = \sqrt{2}\left[1 - \frac{2}{3} + \frac{2.4}{3.5} - \frac{2.4.6}{3.5.7} + \frac{2.4.6.8}{3.5.7.9} - \ldots\right].$$

Les développements de arc sin z et de $(\text{arc sin } z)^2$ donnent, de même,

$$(117)\quad \begin{cases} \operatorname{Log}\dfrac{a^{2r}}{Q^r} = \dfrac{\sqrt{\Delta}\,U_r}{Q^{\frac{r}{2}}}\left[1 - \dfrac{1}{1.2.3}\dfrac{\Delta U_r^2}{2^2 Q^r} + \dfrac{(1.3)^2}{1.2.3.4.5}\dfrac{\Delta^2 U_r^4}{2^4 Q^{2r}} - \ldots.\right], \\ \dfrac{1}{4}\operatorname{Log}^2\dfrac{a^{2r}}{Q^r} = \dfrac{\Delta U_r^2}{2^2 Q^r} - \dfrac{1}{2}\cdot\dfrac{2}{3}\dfrac{\Delta^2 U_r^4}{2^4 Q^{2r}} + \dfrac{1}{3}\cdot\dfrac{2.4}{3.5}\dfrac{\Delta^3 U_r^6}{2^6 Q^{3r}} - \ldots., \end{cases}$$

et, à la limite de convergence,

$$(118)\quad \begin{cases} \operatorname{Log}(1+\sqrt{2}) = 1 - \dfrac{1}{1.2.3} + \dfrac{(1.3)^2}{1.2.3.4.5} - \dfrac{(1.3.5)^2}{1.2.3.4.5.6.7} + \ldots, \\ \operatorname{Log}(1+\sqrt{2}) = 1 - \dfrac{1}{2}\cdot\dfrac{2}{3} + \dfrac{1}{3}\cdot\dfrac{1.4}{3.5} - \dfrac{1}{5}\cdot\dfrac{2.4.6}{3.5.7} + \ldots \end{cases}$$

La formule remarquable de M. SCROLTZ conduit au développement

$$(119)\quad \operatorname{Log}^3\frac{a^{2r}}{Q^r} = \frac{\Delta^{\frac{3}{2}}U_r^3}{Q^{\frac{3r}{2}}}\left[1 - \frac{3.3}{4.5}\left(1+\frac{1}{3^3}\right)\frac{\Delta U_r^2}{2^2 Q^{2r}} + \frac{3.5.3}{4.6.7}\left(1+\frac{1}{3^2}+\frac{1}{5^2}\right)\frac{\Delta^2 U_r^4}{2^4 Q^{2r}} - \ldots\right.$$
$$\left. \pm \frac{3.5.7\ldots(2n-1)3}{4.6.8..2n(2n+1)}\left(1+\frac{1}{3^2}+\frac{1}{5^2}+\ldots\frac{1}{(2n-1)^2}\right)\frac{\Delta^{n-1}U_r^{2n-2}}{2^{2n-2}Q^{(n-1)r}} \mp \ldots\right],$$

et, à la limite de convergence

$$(120)\qquad \operatorname{Log}^3(1+\sqrt{2}) = 1 - \frac{3.3}{4.5}\left(1+\frac{1}{3^3}\right) + \frac{3.5.3}{4.6.7}\left(1+\frac{1}{3^2}+\frac{1}{5^2}\right) - \ldots.$$

Si l'on développe, par la formule de LAGRANGE, l'une des racines a^r ou b^r de l'équation

$$z^2 - zV_r + Q^r = 0\ ,$$

on trouve

$$(121)\quad \begin{cases} b^r = \dfrac{Q^r}{V_r} + \dfrac{Q^{2r}}{V_r^3} + \dfrac{4}{2}\dfrac{Q^{3r}}{V_r^5} + \dfrac{5.6}{2.3}\dfrac{Q^{4r}}{V_r^7} + \ldots\ , \\ \operatorname{Log} b^r = \operatorname{Log}\dfrac{Q^r}{V_r} + \dfrac{Q^r}{V_r^2} + \dfrac{3}{2}\dfrac{Q^{2r}}{V_r^4} + \dfrac{5.4}{2.3}\dfrac{Q^{3r}}{V_r^6} + \ldots\ , \\ \dfrac{1}{3}b^{2r} = \dfrac{Q^{2r}}{2V_r^2} + \dfrac{Q^{3r}}{V_r^4} + \dfrac{5}{2}\dfrac{Q^{4r}}{V_r^6} + \dfrac{7.6}{2.3}\dfrac{Q^{5r}}{V_r^8} + \ldots. \end{cases}$$

Si l'on fait encore, par la formule de LAGRANGE, le développement de y^{-n} suivant les puissances de z, en désignant par y l'une des racines de l'équation

$$y = 2 + \frac{z}{y}\ ,$$

on obtient

$$\left(\frac{2}{1+\sqrt{1+z}}\right)^n = 1 - \frac{n}{1}\frac{z}{4} + \frac{n(n+3)}{1.2}\left(\frac{z}{4}\right)^2 - \frac{n(n+4)(n+5)}{1.2.3}\left(\frac{z}{4}\right)^3 + \frac{n(n+5)(n+6)(n+7)}{1.2.3.4}\left(\frac{z}{4}\right)^4 - \dots ,$$

et en posant

$$\frac{z}{4} = -\frac{Q^r}{V_r^2} ,$$

on a

$$\frac{V_{nr}a^{nr}}{Q^{nr}} = 1 + \frac{n}{1}\frac{Q^r}{V_r^2} + \frac{n(n+3)}{1.2}\frac{Q^{2r}}{V_r^4} + \frac{n(n+4)(n+5)}{1.2.3}\frac{Q^{3r}}{V_r^6} + \dots , \tag{122}$$

cette série est convergente pour $\frac{Q^r}{V_r^2} < 1$; elle contient la généralisation de la formule (84).

On a encore

$$b^r = \frac{V_r - \sqrt{V_r^2 - 4Q^r}}{2} ,$$

et, en développant le radical par la formule du binôme,

$$b^n = \frac{1}{2}\frac{2Q^r}{V_r} + \frac{1}{2.4}\frac{2^3Q^{2r}}{V_r^3} + \frac{1.3}{2.4.6}\frac{2^5Q^{3r}}{V_r^5} + \dots , \tag{123}$$

puis, à la limite de convergence,

$$\sqrt{2} - 1 = \frac{1}{2} - \frac{1}{2.4} + \frac{1.3}{2.4.6} - \frac{2.3.5}{1.4.6.8} + \dots \tag{124}$$

En appliquant la formule de BURMANN au développement de *z* suivant les puissances de $\frac{2z}{1+z^2}$ on obtiendrait, pour tout module de *z* inférieur à l'unité, et faisant ensuite $z = \frac{b^r}{a^r}$, la formule (121) donnée ci-dessus.

SECTION XIX.

Sur le calcul rapide des fractions continues périodiques.

On perfectionne, d'une manière notable, le calcul des réduites des fractions continues périodiques au moyen des formules suivantes. M. CATALAN a donné les relations :

$$\frac{z}{1-z^2}+\frac{z^2}{1-z^4}=\frac{z+z^2+z^4}{1-z^4}\ ,$$

$$\frac{z}{1-z^2}+\frac{z^2}{1-z^4}+\frac{z^4}{1-z^8}=\frac{z+z^2+z^3+z^4+z^5+z^6+z^7}{1-z^8}\ ,$$

$$\frac{z}{1-z^2}+\frac{z^2}{1-z^4}+\frac{z^4}{1-z^8}+\frac{z^4}{1-z^{16}}=\frac{z+z^2+\ldots\ldots+z^{14}+z^{15}}{1-z^{16}}\ ,$$

. . . . . ;

on **a,** plus généralement,

$$\frac{z}{1-z^2}+\frac{z^2}{1-z^4}+\ldots+\frac{z^{2^{n-1}}}{1-z^{2^n}}=\frac{1}{1-z}\cdot\frac{z-z^{2^n}}{1-z^{2^n}}\ ;$$

par conséquent, si l'on fait $z=\frac{b^r}{a^r}$ on obtient la formule

$$\frac{Q^r}{U_{2r}}+\frac{Q^{2r}}{U_{4r}}+\ldots.+\frac{Q^{2^{n-1}.r}}{U_{2^n.r}}=\frac{Q^rU_{(2^n-1)r}}{U_rU_{2^n.r}}\ . \tag{125}$$

Lorsque *n* augmente indéfiniment, on a, pour les séries de première et de seconde espèce,

$$\frac{b^r}{U_r}=\frac{Q^r}{U_{2r}}+\frac{Q^{2r}}{U_{4r}}+\frac{Q^{4r}}{U_{8r}}+\ldots.. \tag{126}$$

Par exemple, dans la série de FIBONACCI, pour r = 1 ,

$$\frac{1-\sqrt{5}}{2}=-\frac{1}{2}+\frac{1}{3}+\frac{1}{3\,.\,7}+\frac{1}{3\,.\,7\,.\,47}+\frac{1}{3\,.\,7\,.\,47\,.\,2207}+\ldots\ ; \tag{127}$$

chacun des nouveaux facteurs des dénominateurs est égal au carré du précédent, diminué de deux unités ; de même, dans la série de PELL,

$$1-\sqrt{2}=-\frac{1}{2}+\frac{1}{2^2\,.\,3}+\frac{1}{2^3\,.\,3\,.\,17}+\frac{1}{2^4\,.\,3\,.\,17\,.\,577}+\ldots\ ; \tag{128}$$

chacun des nouveaux facteurs des dénominateurs est égal, par les formules de duplication, au double du carré du précédent, diminué de l'unité.

Ces développements sont très-rapidement convergents ; c'est, en quelque sorte, la combinaison du calcul logarithmique et du calcul par les fractions continues. Ainsi le dénominateur de la trentième-deuxième fraction de la formule (127), est à peu près égal à

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{2^{32}}\ ,$$

et contient *deux-cent millions de chifres,* environ ; pour écrire le dénominateur de la soixante-quatrième fraction de la formule (128), il faudrait plus de *deux-cent millions de siècles.*

Nous avons d'ailleurs démontré (Section XI), que les différents facteurs des dénominateurs sont premiers entre eux deux à deux, et contiennent, par conséquent, des facteurs premiers tous différents ; il en résulte que dans la somme des n premiers termes de ces séries, il n'y aura pas lieu de réduire cette somme à une plus simple expression. Nous montrerons, de plus, que tous ces facteurs, premiers et différents, appartiennent à des formes, linéaires et quadratiques, déterminées.

On a, plus généralement, l'identité

$$\text{(129)} \qquad \frac{z-z^q}{(1-z)(1-z^q)}+\frac{z^q-z^{pq}}{(1-z^q)(1-z^{pq})}=\frac{z-z^{pq}}{(1-z)(1-z^{pq})} \ ;$$

si l'on remplace q par p^n, on a donc

$$\text{(130)} \qquad \frac{z-z^{p^n}}{(1-z)(1-z^{p^n})}+\frac{z^{p^n}-z^{p^{n+1}}}{(1-z^{p^n})(1-z^{p^{n+1}})}=\frac{z-z^{p^{n+1}}}{(1-z)(1-z^{p^{n+1}})} \ .$$

Si l'on fait successivement n égal à 1, 2, 3, . . . n, et si l'on ajoute les égalités obtenues, on a

$$\text{(131)} \qquad \frac{z-z^p}{(1-z)(1-z^p)}+\frac{z^p-z^{p^2}}{(1-z^p)(1-z^{p^2})}+\frac{z^{p^2}-z^{p^3}}{(1-z^{p^2})(1-z^{p^3})}+\ldots + \frac{z^{p^n}-z^{p^{n+1}}}{(1-z^{p^n})(1-z^{p^{n+1}})}=\frac{z-z^{p^{n+1}}}{(1-z)(1-z^{p^{n+1}})} \ .$$

Faisons maintenant $z=\frac{b^r}{a^r}$ nous obtenons la formule

$$\text{(132)} \qquad \frac{Q^r U_{(p-1)r}}{U_r U_{pr}}+\frac{Q^{pr}U_{(p-1)pr}}{U_{pr}U_{p^2r}}\frac{Q^{p^2r}U_{(p-1)p^2r}}{U_{p^2r}U_{p^3r}}+\ldots+\frac{Q^{p^nr}U_{(p-1)p^nr}}{U_{p^nr}U_{p^{n+1}r}}=\frac{Q^rU_{(p^{n+1}-1)r}}{U_rU_{p^{n+1}r}} \ .$$

On calculera d'ailleurs les numérateurs et les dénominateurs de ces fractions, au moyen des formules de multiplication des fonctions numériques que nous avons données. Si p désigne un nombre impair, on obtient une formule analogue en changeant U en V. On peut encore appliquer ces formules aux fonctions circulaires.

Nous donnerons plus tard les formules analogues que l'on déduit de la théorie des fonctions elliptiques, et, en particulier, les sommes des inverses des termes U_n et de leurs puissances semblables.

SECTION XX.

Des relations des fonctions U_n et V_n avec la théorie de l'équation binôme.

On sait, par la théorie de l'équation binôme, exposée dans la dernière section des *Disquisitiones Arithmeticæ*, que si p désigne un nombre premier impair, le quotient $4\dfrac{z^p-1}{z-1}=4(z^{p-1}+z^{p-2}+z^{p-3}+\ldots+z^2+z+1)$

peut être écrit sous la forme $4\dfrac{z^p-1}{z-1}=Y^2\pm pZ^2$,

dans laquelle Y *et* Z sont des polynomes en z à coefficients entiers ; on prend le signe + lorsque p désigne un nombre premier de la forme $4q+3$, et le signe –, lorsque p désigne un nombre premier de la forme $4q+1$. Si l'on fait dans cette formule $z=\sqrt{\dfrac{a^r}{b^r}}$ on en déduit successivement pour $p = 3, 5, 7, 11, 13\ 17, 19, 23, 29, \ldots\ldots$, les résultats suivants :

(133)
$$
\left\{\begin{aligned}
&4\frac{U_{3r}}{U_r}=\Delta U_r^2+3Q^r\ ,\\
&4\frac{U_{5r}}{U_r}=\left[2V_{2r}+Q^r\right]^2-5Q^{2r}\ ,\\
&4\frac{U_{7r}}{U_r}=\Delta\left[2U_{3r}+Q^rU_r\right]^2+7Q^{2r}V_r^2\ ,\\
&4\frac{U_{11r}}{U_r}=\Delta\left[2U_{5r}+Q^rU_{3r}-24Q^{2r}U_r\right]^2+11Q^{2r}V_{3r}^2\ ,\\
&4\frac{U_{13r}}{U_r}=\left[2V_{6r}+Q^rV_{4r}+4Q^{2r}V_{2r}-Q^{3r}\right]^2-13Q^{2r}\left[V_{4r}+Q^{2r}\right]^2\ ,\\
&4\frac{U_{17r}}{U_r}=\left[2V_{8r}+Q^rV_{6r}+5Q^{2r}V_{4r}+7Q^{3r}V_{2r}+4Q^{4r}\right]^2-17Q^{2r}\left[V_{6r}+Q^rV_{4r}+Q^{2r}V_{2r}+2Q^{3r}\right]^2,\\
&4\frac{U_{19r}}{U_r}=\Delta\left[2U_{9r}+Q^rU_{7r}-4Q^{2r}U_{5r}+3Q^{3r}U_{3r}+5Q^{4r}U_r\right]^2\\
&\qquad\qquad+19Q^{2r}\left[V_{9r}+Q^rV_{7r}-Q^{3r}V_{3r}-2Q^{4r}V_r\right]^2,\\
&4\frac{U_{23r}}{U_r}=\Delta\left[2U_{11r}+Q^rU_{9r}-5Q^{2r}U_{7r}-8Q^{3r}U_{5r}-7Q^{4r}U_{3r}-4Q^{5r}U_r\right]^2\\
&\qquad\qquad+23Q^{2r}\left[V_{9r}+Q^rV_{7r}-Q^{3r}V_{3r}-2Q^{4r}V_r\right]^2\ ,\\
&4\frac{U_{29r}}{U_r}=\left[2V_{14r}+Q^rV_{12r}+8Q^{2r}V_{10r}-3Q^{3r}V_{8r}+Q^{4r}V_{6r}-2Q^{5r}V_{4r}+3Q^{6r}V_{2r}\right.\\
&\qquad\qquad\left.+9Q^{7r}\right]^2-29Q^{2r}\left[V_{12r}+Q^{2r}V_{8r}-Q^{3r}V_{6r}+Q^{5r}V_{2r}+Q^{5r}\right]^2\ ,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}\right.
$$

On a, par conséquent, la proposition suivante :

THEOREME : *Si p désigne un nombre premier de la forme* $4q+1$, *le quotient* $4\frac{U_{pr}}{U_r}$ *peut se mettre sous la forme* Y^2-pZ^2, *et si p désigne un nombre premier de la forme* $4q+3$, *le quotient* $4\frac{U_{pr}}{U_r}$ *peut se mettre sont la forme* ΔY^2-pZ^2.

D'ailleurs, en changeant z en $-z$, on obtiendra un résultat semblable pour le quotient $4\frac{V_{pr}}{V_r}$. On généralise ainsi un théorème donné par LEGENDRE, et dont la démonstration est, de cette façon, rendue plus simple. Il résulte encore des formules (133) une autre conséquence importante. En effet, nous avons laissé jusqu'à présent Δ arbitraire ; mais, s'il s'agit des fonctions de troisième espèce, nous pouvons supposer $-\Delta$ égal au produit d'un carré par un nombre premier p de la forme $4q+3$;* alors, on voit que les quotients $4\frac{U_{pr}}{pU_r}$ et $4\frac{V_{pr}}{pV_r}$ sont égaux à une différence de carrés, et, par suite, décomposables en un produit de deux facteurs. On a donc cette proposition :

THEOREME : *Si* $-\Delta$ *est égal au produit d'un nombre premier p de la forme* $4q+3$ *par un carré, les quotients* $4\frac{U_{pr}}{pU_r}$ *et* $4\frac{V_{pr}}{pV_r}$ *sont, quelle que soit la valeur entière de r, décomposables en un produit de deux facteurs entiers.*

Si nous considérons l'équation fondamentale

$$x^2 = x - 2$$

dans laquelle $\Delta = -7$, nous obtenons, par exemple,

$$U_{11} = +23, \quad U_{77} = -26\,4721893121 ;$$

et, par suite,

$$U_{77} = -7 \times 23 \times 11087 \times 148303.$$

Nous démontrerons plus loin que les diviseurs premiers de $\frac{4U_n}{7U_{11}}$ appartiennent aux formes linéaires $77q \pm 1$; par conséquent, le nombre 11087 est premier, sans qu'il soit nécessaire d'essayer ces diviseurs, puisque le premier des nombres de la forme linéaire indiquée, est supérieur à la racine carrée de 11087 ; pour le facteur 148303 il n'y a que le diviseur 307 à essayer. On a encore, dans la même série

* En effet, il suffit de déterminer Q par la relation $4Q-P^2 = pK^2$.

$$U_{13} = -1, \qquad U_{91} = -\ 384\ 17168\ 38057,$$

et, par suite,

$$U_{91} = -\ 7 \times 712711 \times 770041.$$

Ces deux derniers facteurs sont premiers ; il n'y a que deux diviseurs à essayer. On comprend ainsi comment il est possible d'appliquer le théorème précédent, à la recherche directe de très-grands nombres premiers, par la considération des séries de troisième espèce.

SECTION XXI.

Sur les congruences du Triangle Arithmétique de PASCAL, et sur une géneralisation du théorème de FERMAT.

En désignant par C_m^n le nombre des combinaisons de m objets pris n à n, on a les deux formules fondamentales

$$C_m^n = \frac{m(m-1)\ldots.(m-n+1)}{1.2.3\ldots.n}$$

$$C_m^n = C_{m-1}^n + C_{m-1}^{n-1}\ ;$$

par conséquent, lorsque p est premier, on a pour n entier compris entre 0 et la congruence

(134) $$C_p^n \equiv 0, \quad (\text{Mod. } p)\ ;$$

pour n compris entre 0 et $p - 1$,

(135) $$C_{p-1}^n \equiv (-1)^n, \quad (\text{Mod. } p)\ ;$$

pour n compris entre 1 et p

(136) $$C_{p+1}^n \equiv 0, \quad (\text{Mod. } p)\ .$$

En d'autres termes, dans le triangle arithmétique de PASCAL, tous les nombres de la $p^{ième}$ ligne sont, pour p premier, divisibles par p, à l'exception des coefficients extrêmes égaux à l'unité ; les coefficients de la $(p-1)^{ième}$ ligne donnent alternativement pour résidus + 1 et – 1; ceux de la $(p+1)^{ième}$ ligne sont divisibles par p, en exceptant les quatre coefficients extrêmes, égaux à l'unité.

Si l'on continue la formation du triangle arithmétique, en ne conservant que les résidus suivant le module p, on reforme deux fois le triangle arithmétique des $(p-1)$ premières lignes ; puis, à partir de la $(2p)^{ième}$ ligne, on le reforme trois fois ; mais les résidus du triangle intermédiaire sont multipliés par 2 ; à partir de la $(3p)^{ième}$ ligne, le triangle des résidus est reproduit quatre fois, mais les nombres de ces triangles sont respectivement multipliés par les

coefficients 1, 3, 3, 1 de la troisième puissance du binôme, et ainsi de suite.

On a donc, en général,

$$C_m^n \equiv C_{m_1}^{n_1} \times C_\mu^\nu , \quad (\text{Mod. } p),$$

m_1 et n_1 désignant les entiers de $\frac{m}{p}$ et de $\frac{n}{p}$, et μ et et **v** les résidus de m et de n.

On a, de même

$$C_{m_1}^{n_1} \equiv C_{m_2}^{n_2} \times C_{\mu_1}^{\nu_1} , \quad (\text{Mod. } p),$$

et, par suite,

(137) $$C_m^n \equiv C_{\mu_1}^{\nu_1} \times C_{\mu_2}^{\nu_2} \times C_{\mu_3}^{\nu_3} \times \ldots , \quad (\text{Mod. } p),$$

μ_1, μ_2, μ_3, ... désignant les résidus de m et des entiers de $\frac{m}{p}, \frac{m}{p^2}, \frac{m}{p^3}$, ... ,et de même pour ν_1, ν_2, ν_3, ...

Par conséquent, si l'on veut trouver le reste de la division de C_m^n par un nombre premier, il suffit d'appliquer la formule précédente, jusqu'à ce qu'on ait ramené les deux indices de C, à des nombres inférieurs à p.

Nous venons de voir que les coefficients de la puissance p du binôme sont entiers et divisibles par p, lorsque p désigne un nombre premier, en exceptant toutefois les coefficients des puissances $p^{ièmes}$. En désignant par α, β, γ, ... λ, des entiers quelconques, en nombre n, on a donc

$$[\alpha + \beta + \gamma + \ldots . + \lambda]^p - [\alpha^p + \beta^p + \gamma^p + \ldots . + \lambda^p] \equiv 0 , \quad (\text{Mod. } p),$$

et, pour $\alpha = \beta = \gamma \ldots = \lambda = 1$, on obtient

$$n^p - n \equiv 0 , \quad (\text{Mod. } p) .$$

C'est dans cette congruence que consiste le théorème de FERMAT, que l'on peut généraliser de la manière suivante, différente de celle que l'on doit à EULER. Si α, β, γ, . . . λ, désignent les puissances $q^{ièmes}$ des racines d'une équation à coefficients entiers, et S_q leur somme, le premier membre de la congruence précédente représente le produit par p d'une fonction symétrique, entière et à coefficients entiers, des racines, et, par conséquent, des coeflicients de l'équation proposée. On a donc

$$S_{pq} \equiv S_q^p , \quad (\text{Mod. } p) ,$$

et, par l'application du théorème de FERMAT,

(138) $$S_{pq} \equiv S_q , \quad (\text{Mod. } p) ,$$

L'étude des diviseurs premiers de la fonction numérique S_n et de quelques autres analogues est trés-importante ; on a, en particulier, pour $n = 1$ et $S_1 = 0$, comme dans l'équation

$$x^3 = x + 1 ,$$

la congruence

$$S_p \equiv 0, \quad (\text{Mod. } p) ;$$

on en déduit inversement que *si, dans le cas de* $S_1 = 0$, *on a* S_n *divisible par* p, *pour* $n = p$, *et non auparavant, le nombre* p *est un nombre premier*. En effet, supposons p égal, par exemple, au produit de deux nombres premiers g et h. On a

$$S_{gh} \equiv S_h , \quad (\text{Mod. } g) ,$$

$$S_{gh} \equiv S_g , \quad (\text{Mod. } h) ;$$

par conséquent, si l'on a trouvé

$$S_{gh} \equiv 0, \quad (\text{Mod. } gh) ,$$

on aura aussi

$$S_g \equiv 0, \quad (\text{Mod. } h) ,$$

$$S_h \equiv 0, \quad (\text{Mod. } g) ,$$

et, par le théorème démontré

$$S_g \equiv S_h \equiv 0, \quad (\text{Mod. } gh) .$$

Ainsi S_{gh} ne serait pas le premier des nombres S_n divisible par gh.

On peut obtenir, de cette façon, un grand nombre de théorèmes servant, comme celui de WILSON, à vérifier les nombres premiers. Nous laisserons de côté, pour l'instant, les développements curieux et nouveaux que nous avons ainsi trouvés, pour ne considérer que ceux que l'on tire des fonctions numériques simplement périodiques.

SECTION XXII.

Sur la théorie des nombres premiers dans leurs rapports avec les progressions arithmétiques.

La doctrine des nombres premiers a été ébauchée par EUCLIDE et ERATOSTHENE. On doit à Euclide la théorie des diviseurs et des multiples communs de deux ou plusieurs nombres donnés, la représentation des nombres composés à l'aide de leurs facteurs, et la démonstration de l'infinité des nombres premiers, que l'on peut étendre facilement à la preuve de l'infinité des nombres premiers appartenant aux formes linéaires $4x + 3$ et $6x + 5$. Nous donnerons, dans la Section XXIV, une démonstration élémentaire concernant l'infinité des nombres premiers de la forme $mx + 1$, quelle que soit la valeur de m. On sait d'ailleurs que, par l'emploi des séries infinies, LEJEUNE-DIRICHLET est parvenu à démontrer l'infinité des nombres premiers

de la forme linéaire $a + bx$, dans laquelle a et b sont deux entiers quelconques premiers entre eux.[*]

On doit à ERATOSTHENE une méthode ingénieuse connue sous le nom de *Crible Arithmétique*, qui conduit à la formation de la table des nombres premiers et des nombres composés ; on possède, depuis les travaux de CHERNAC, de BURCKHARDT et de DASE, la table des neuf premiers millions ; LEBESGUE a indiqué un procédé qui permet de diminuer le volume de ces tables.[†] D'autre part, M. GLAISHER a évalué la multitude des nombres premiers compris dans ces tables, afin de comparer les formules théoriques données par GAUSS, LEGENDRE, TCHEBYCHEF et HEARGRAVE, pour exprimer la quantité des nombres premiers inférieurs à un entier donné. M. GLAISHER, en comptant 1 et 2 comme premiers, a trouvé les valeurs suivantes :[‡]

pour le premier million,			78499	nombres premiers ,	
"	deuxième	" ,	70433	"	,
"	troisième	" ,	67885	"	,
"	septième	" ,	63799	"	,
"	huitième	" ,	63158	"	,
"	neuvième	" ,	62760	"	.

Les principes d'EUCLIDE et d'ERATOSTHENE conduisent ainsi à une première méthode de vérification des nombres premiers, non compris dans les Tables, et de décomposition des nombres très-grands en leurs facteurs premiers, par l'essai successif de la division d'un nombre *fixe*, le nombre donné, par tous les nombres premiers inférieurs à sa racine carrée. Mais c'est là une méthode indirecte qui devient absolument impraticable, dès que le nombre donné a dix chiffres.

En suivant cette voie, M. DORMOY est arrivé par des considérations ingénieuses, déduites de la théorie de certains nombres, qu'il a appelés *objectifs* (et dans lesquels on retrouve sous le nom *d'objectifs de l'unité* les différents termes de la série de FIBONACCI), à l'établissement d'une formule générale de nombres premiers. Malheureusement, même pour des limites peu élevées, cette formule contient des coefficients considérables qui en rendent l'application illusoire.[§]

---

[*] *Abhandlungen der Berliner Akademie,* Berlin, 1837.

[†] CHERNAC. – *Criblum Arithmeticum* de l à 1020000. Deventer, 1811.
BURCKHARDT. – *Tables des diviseurs* jusqu'à 3036000. Paris, 1814-1817.
DASE. – *Factorem Tafeln* de 6000000 à 9000000. Vienne, 1862-1865.
LEBESGUE. – *Tables diverses pour la décomposition des nombres en leurs facteurs premiers.* Paris,1864.

[‡] *Preliminary accounts of the results of an enumeration of the primes in Dase's and Burckhardt's tables.* Cambridge, 1876-1877.

[§] E. DORMOY. – *Formule générale des nombres premiers et Théorie des Objectifs.* Paris, 1867.

Les nombres premiers sont distribués fort irrégulièrement dans la suite des nombres entiers ; c'est qu'en effet, d'une part, on voit que si μ désigne le plus petit multiple commun des nombres 2, 3, ... m, les nombres

$$\mu + 2, \mu + 3, \ldots, \mu + m ,$$

sont respectivement divisibles par

$$2, 3, \ldots m .$$

Par conséquent, on peut toujours trouver m nombres consécutifs et composés, quelle que soit la valeur de m ; mais, d'autre part, l'examen des tables permet de constater l'existence de deux nombres impairs consécutifs, très-grands, et premiers. M. GLAISHER a donné la liste des groupes, renfermés dans les tables, qui contiennent au moins cinquante nombres consécutifs et composés ; ainsi, par exemple, les suivants :

111	nombres composés et consécutifs entre		370261	et	370373,
113	"	"	492113	et	492227,
131	"	"	1357201	et	1357333,
131	"	"	1561919	et	1562051,
147	"	"	2010733	et	2010881,

(*London Mathematical Society*, 10 Mai, 1877).

On sait encore démontrer qu'une fonction rationnelle de n

$$p = \phi(n) ,$$

ne peut continuellement donner des nombres premiers, puisque l'on a, quelque soit le nombre entier k,

$$\phi(n + kp) \equiv \phi(n), \ (\text{Mod. } p) ,$$

c'est-à-dire que $\phi(n)$ est une fonction numérique périodique d'amplitude p. Il est donc fort difficile d'arriver à la loi de distribution des nombres premiers dans la série ordinaire des nombres entiers.

Cependant, il parait naturel d'étudier les nombres premiers d'après leur loi de formation. L'étude approfondie de la méthode d'ERATOSTHENE a conduit le prince A. DE POLIGNAC, à d'intéressantes propriétés des *suites diatomiques* ;[*] à la même époque, M. TCHEBYCHEF, arrivait par des considérations peu ditrérentes, à la démonstration de ce théorème remarquable : *Pour* $a > 3$, *il y a au moins un nombre premier compris entre* a *et* $2a - 2$.[†] On déduit immédiatement de là que le produit

$$1.2.3 \ldots . n$$

[*] *Recherches nouvelles sur les nombres premiers* ; par M. A. DE POLIGNAC ; Paris, 1851. Il est curieux de constater que, sous le nom de *suite médiane*, on retrouve dans les séries diatomiques, les différents terme de la série de FERMAT.

[†] *Journal de Liouville*, t. XVII.

ne saurait être une puissance, ni un produit de puissances, ainsi que l'a montré M. LIOUVILLE. (*Journal de Liouville*, 2[e] série, t. II). En résumé, ces recherches sont basées sur la *considération des progressions arithmétiques.*

SECTION XXIII.

Sur la théorie des nombres premiers dans leurs rapports avec les progressions géométriques.

On doit à FERMAT des recherches profondes sur la théorie des nombres premiers, et basées sur la considération des *progressions géométriques.* C'est cette idée, distincte de la précédente, qui a donné naissance à la *théorie des résidus potentiels*, et plus particulièrement, à celle des *résidus quadratiques.* De cette façon, on simplifie la vérification des nombres premiers très-grands, et diviseurs de la forme a^n-1 ou plus généralement, de la forme a^n-b^n, pour a et b entiers, ainsi que la décomposition des nombres de cette forme en facteurs premiers. FERMAT avait remarqué la forme linéaire $nx+1$ des diviseurs, et donné lui-même la décomposition de plusieurs termes de la série 2^n-1, et ainsi, celle du nombre $2^{37}-1$, qu 'il a trouvé divisible par 223 [*Lettre de* FERMAT, du 12 Octobre 1640].

M. GENOCCHI a remis dernièrement en lumière un curieux passage des oeuvres du P. MERSENNE. Mais, pour en mieux saisir l'importance, nous rappellerons en quelques mots la théorie des *nombres parfaits.* On dit qu'un nombre est *parfait,* lorsque il est égal à la somme de ses parties *aliquotes,* c'est à-dire de tous ses diviseurs, excepté lui-même. En nous bornant au cas des nombres parfaits pairs, et en désignant par b, c, ... d es nombres premiers différents, par $n=a^\alpha b^\beta c^\gamma d^\delta$ . . . . le nombre supposé parfait, on doit avoir

$$2^{\alpha+1}b^\beta c^\gamma\ldots = (1 + 2 + \ldots +2^\alpha)(1 + b + b^2 + \ldots + b^\beta)\ (1 + c + c^2 + \ldots + c^\gamma)\ldots ,$$

ou bien

$$b^\beta c^\gamma\ldots+\frac{b^\beta c^\gamma\ldots}{2^{\alpha+1}-1}=(1+b+b^2+\ldots+b^\beta)(1+c+c^2+\ldots+c^\gamma)\ldots . ;$$

le second terme du premier membre est donc entier, et devient, après la division, de la forme $b^{\beta'}c^{\gamma'}\ldots$; mais d'autre part, le second membre qui contient un nombre de termes

$$\mu = (\beta + 1)(\gamma + 1) \ldots . ,$$

doit se réduire aux deux termes du premier membre ; par suite $\mu = 2$, $\beta = 1$, $\gamma = \delta = \ldots . = 0$; donc $n=2^\alpha b$, et b est premier. Ainsi, les nombres parfaits

pairs appartiennent à la forme $n = 2^{\alpha} b$, dans laquelle b doit être premier ; on a d'ailleurs aisément, avec cette condition

$$b = 2^{\alpha+1} - 1 \ .$$

En résumé, il n'y a pas d'autres nombres parfaits pairs que les nombres

$$2^{\alpha}\left(2^{\alpha+1} - 1\right) ,$$

dans lesquels le second facteur est un nombre premier. Cette règle était connue d'EUCLIDE ; mais ce géométre ne savait pas démontrer que l'on obtenait ainsi tous les nombres parfaits pairs, sans exception.

Voici maintenant le passage des Œuvres de MERSENNE :

« XIX. Ad ea quæ de Numeris ad calcem prop. 20. de Ballist. & puncto 14 Præfationis ad Hydraul. dicta sunt, adde inuentam artem quâ numeri, quotquot volueris, reperiantur qui cum suis partibus aliquotes in vnicam summam redactis, non solum duplam rationem habeant, (quales sunt 120, minimus omnium, 672, 528776, 1416304896, & 459818240, qui ductus in 3, numerum efficit 1379454120, cuius partes aliqnotæ triplæ sunt, quales etiam sequentes 30240, 32760, 23569920, & alij infiniti, de quibus videatur Harmonia nostra, in qua 14182439040, & alij suarum partium aliquotarum subquadrupli) sed etiam sint in ratione data cum suis partibus aliquotis.

Sunt etiam alij numeri, quos vocant amicabiles, quod habeant partes aliquotas à quibus mutuò reficiantur, quales sunt omnium minimi 220, & 284 ; huius enim aliquotæ partes illum efficiunt, vicéque versa partes illius aliquotæ hunc perfectè restituunt. Quales & 18416 & 17296 ; nec non 9437036, & 4363584 reperies, aliosque innumeros.

Vbi fuerit operæ pretium aduertere XXVIII numeros à Petro Bungo pro pertectis exhibitos, capite XXVIII, libri de Numeris, non esse omnes Perfectos, quippe 20 sunt imperfecti, adeo vt solos octo perfectos habeat videlicet 6. 28. 499. 8128. 33550336. 8589869056. 137438691328, & 2805843008139952128 ; qui sunt è regione tabulæ Bungi, 1, 2, 3, 4, 8, 10, 12, & 29 : quique soli perfecti sunt, vt qui Bungum habuerint, érrori medicinam faciant.

Porrò numeri perfecti adeo rari sunt, vt vndecim dumtaxat potuerint hactenus inueniri : hoc est, alii tres à Bougianis differentes : neque enim vllus est alius perfectus ab illis octo, nisi superes exponentem numerum 62, progressionis duplæ ab 1 incipientis. Nonus enim perfectus est potestas exponentis 68 minus 1. Decimus, potestas exponentis 128, minus 1. Vndecimus denique, potestas 258, minus 1, hoc est potestas 257, vnitate decurtata, multiplicata per potestatem 256.

Qui vndecim alios repererit, nouerit se analysim omnem, quæ fuerit hactenus, superasse : memineritque interea nullum esse perfectum à 17000 potestate ad 32000 ; & nullum potestatum interuallum tantum assignari posse, quin detur illud absque perfectis. Verbi gratia, si fuerit exponens 1050000, nullus erit numerus progressionis duplæ vsque ad 2090000, qui perfectis numeris serviat, hoc est qui minor vnitate, primus existat.

« Vnde clarum est quàm rari sint perfecti numeri, & quàm meritò viris perfectis comparentur ; esseque vnam ex maximis totius Matheseos difficultatibus, præscriptam numerorum perfectorum multitudinum exhibere ; quemadmodum & agnoscere num dati numeri 15, aut 20 caracteribus constantes, sint primi necne, cùm nequidem sæculum integrum huic examini, quocumque modo hactenus cognito, sufficiat. »[*]

[*] F. MARINI MERSENNI MINIMI, COGITATA PHYSICO-MATHEMATICA. *In quibus tam naturæ quàm*

D'après ce passage, le tableau des nombres parfaits pairs serait le suivant :

Premier nombre parfait	$2(2^2-1)$,	Deuxième nombre parfait	$2^2(2^2-1)$,
Troisième "	$2^4(2^5-1)$,	Quatrième "	$2^6(2^7-1)$,
Cinquième "	$2^{12}(2^{13}-1)$,	Sixième "	$2^{16}(2^{17}-1)$,
Septième "	$2^{18}(2^{19}-1)$,	Huitième "	$2^{30}(2^{31}-1)$,
Neuvième "	$2^{66}(2^{67}-1)$,	Dixième "	$2^{126}(2^{127}-1)$,
Onzième "	$2^{256}(2^{257}-1)$,	. . . . .	

Ce passage est d'ailleurs rapporté dans un mémoire de C. N. WINSHEIM, inséré dans les *Novi Commentarii Academiæ Petropolitanæ, ad* annum MDCCXLIX (tom. II, pag. 78), et précédé des réflexions suivantes :

« Suspicio enim adesse videtur, utrum numerus nonus, perfecti locum tueri possit, quoniam ab acutissimo Mersenno exclusus reperitur, qui ejus in locum potestatem binarii $(2^{67}-1)2^{66}$ sive numerum decimum nonum perfectum Hanschii 1 | 47573 | 95258 | 96764 | 12927, substituit : digna certe mihi visa sunt verba viri perspicacissimi, ut hic integra exhibeantur. »

Ainsi MERSENNE aurait démontré que, pour n compris entre 31 et 257, il n'existe pas de nombres premiers de la forme $2^n - 1$, en exceptant ceux pour lesquels n a pour valeur l'un des nombres

$$31,\ 67,\ 127,\ 257.$$

La preuve de non-décomposition du premier de ces nombres, $2^{31} - 1$, n'a été donnée que plus tard, par EULER. En outre, M. F. LANDRY, au moyen d'une méthode inédite, et probablement fort simple, est parvenu à la décomposition de certains grands nombres en leurs facteurs premiers ; il a, en effet, donné la décomposition des nombres

$$2^{41}-1,\quad 2^{43}-1,\quad 2^{47}-1,\quad 2^{53}-1,\quad 2^{59}-1,$$

en leurs facteurs premiers. De plus, on a trouvé que $2^{73}-1$, $2^{79}-1$,et $2^{113}-1$, sont respectivement divisibles par 439, 2687 et 3391. Enfin, on a le théorème suivant :

THEOREME : *Si* $4q+3$ *et* $8q+7$ *sont des nombres premiers, le nombre* $2^{4q+3}-1$ *est divisible par* $8q+7$.

En effet, d'après le thoérème de FERMAT, on a

$$2^{8q+6}-1\equiv 0,\ \text{(Mod. } 8q+7),$$

et, par suite l'un des deux facteurs $2^{4q+3}+1$ ou $2^{4q+3}-1$ du premier membre de la congruence est divisible par le module ; mais, d'autre part, on sait que 2 est résidu quadratique de tous les nombres premiers de l'une des formes $8n+1$ et $8n+7$; par conséquent, on a

$$2^{4q+3}-1\equiv 0,\quad \text{(Mod. } 8q+7);$$

---

artis effectus admirandi certissimis demonstrationibus explicantur. Paris, 1644. f° II.de la Préface.

en consultant la table des nombres premiers, on en conclut que pour les valeurs de n successivement égales à

11, 23, 83, 131, 179, 191, 239, 251, 359, 419, 431, 443, 491,

les nombres $2^n - 1$ sont respectivement divisibles par les facteurs

23, 47, 167, 263, 359, 383, 479, 503, 719, 839, 863, 887, 983.

Il résulte de ces diverses considérations que MERSENNE était en possession d'une méthode arithmétique qui ne nous est point parvenue. Cependant, il paraît naturel de penser que cette méthode ne devait pas s'éloigner des principes de FERMAT, et par conséquent, ne pas différer essentiellement de celle que nous déduirerons, plus loin, de l'inversion du théorème de FERMAT. Nous indiquons, en effet, comment il est possible d'arriver rapidement à l'étude du mode de composition des grands nombres dont il est parlé plus haut.

Nous donnons dans le tableau suivant, la décomposition des nombres U_n et V_n de la série de FERMAT, pour toutes les valeurs de n jusqu'à 64. Parmi les grands nombres premiers de ce tableau, on remarquera

1°. Cinq nombres de dix chiffres

4278255361	facteur de $2^{40}+1$,
8831418697	" $2^{41}+1$,
2931542417	" $2^{44}+1$,
1824726041	" $2^{59}+1$,
4562284561	" $2^{60}+1$;

2°. Deux nombres de onze chiffres

5 44109 72897	facteur de $2^{56}+1$,
7 7158 6 73929	" $2^{63}+1$;

3°. Un nombre de douze chiffres

16 57685 37521	facteur de $2^{47}+1$;

4°. Quatre nombres de treize chiffres

293 20310-07403	facteur de $2^{43}+1$,
443 26767 98593	" $2^{49}-1$,
436 39531 27297	" $2^{49}+1$,
3203431780337	" $2^{59}-1$;

5°. Un nombre de quatorze chiffres

$$2805\ 98107\ 62433 \qquad \text{facteur de} \quad 2^{53}+1.$$

Il reste à déterminer la nature des trois nombres $2^{61}-1$, $\frac{1}{3}(2^{61}+1)$, et $2^{64}+1$. M. LANDRY pense que ces nombres sont premiers ; mais, d'autre part, d'après MERSENNE, le premier de ces nombres serait composé ; de plus, par la considération de calculs que j'ai effectués, et dont la théorie est indiquée plus loin, le dernier de ces nombres serait aussi composé. Il n'y a donc pas lieu de se prononcer pour le moment.

En dehors des décompositions renfermées dans le tableau, M. LANDRY a encore obtenu les diviseurs propres d'un certain nombre d'autres termes de cette série, à savoir

Pour	$2^{65}+1$	4 09891	et	76 23851,
	$2^{69}+1$	16 87499 65921,		(premier) ,
	$2^{71}+1$	1 00801	et	105 67201,
	$2^{75}+1$	113 38367 30401,		(premier) ,
	$2^{105}+1$	6 64441	et	15 64921.

De son côté, M. LE LASSEUR est parvenu aux mêmes résultats ; mais, il a, en outre, indiqué l'identité

$$2^{4n+2}+1 = (2^{2n+1} + 2^{n+1} + 1)\,(2^{2n+1} - 2^{n+1} + 1)$$

qui permet d'abréger les calculs. Cette identité, fort importante, sera généralisée ultérieurement.

TABLEAU DES FACTEURS PREMIERS DE LA SERIE RECURENTE DE FERMAT.

D'après M. F. LANDRY

U_n	Diviseurs de U_n		Valeurs de 2^n	V_n	Diviseurs de V_n
2^1-1	1	2^1	2	2^1+1	3
		2^2	4	2^2+1	5
2^3-1	7	2^3	8	2^3+1	3^2
		2^4	16	2^4+1	17
2^5-1	31	2^5	32	2^5+1	3.11
		2^6	64	2^6+1	5.13
2^7-1	127	2^7	128	2^7+1	3.43
		2^8	256	2^8+1	257
2^9-1	7.73	2^9	512	2^9+1	3^3.19
		2^{10}	1094	$2^{10}+1$	5^2.41
$2^{11}-$	23.89	2^{11}	2048	$2^{11}+1$	3.683
		2^{12}	4096	$2^{12}+1$	17.241
$2^{13}-1$	8191	2^{13}	8192	$2^{13}+1$	3.2731
		2^{14}	16384	$2^{14}+1$	5.29.113
$2^{15}-1$	7.31.151	2^{15}	32768	$2^{15}+1$	3^2.11.331
		2^{16}	65536	$2^{16}+1$	65537
$2^{17}-1$	131071	2^{17}	131072	$2^{17}+1$	3.43691
		2^{18}	262144	$2^{18}+1$	5.13.37.109
$2^{19}-1$	524287	2^{19}	524288	$2^{19}+1$	3.174763
		2^{20}	1048576	$2^{20}+1$	17.61681
$2^{21}-1$	7^2.127.337	2^{21}	2097152	$2^{21}+1$	3^2.43.5419
		2^{22}	4194304	$2^{22}+1$	5.397.2113
$2^{23}-1$	47.178481	2^{23}	8388608	$2^{23}+1$	3.2796203
		2^{24}	16777216	$2^{24}+1$	97.257.673
$2^{25}-1$	31.601.1801	2^{25}	33554432	$2^{25}+1$	3.11.251.4051
		2^{26}	67108864	$2^{26}+1$	5.53.157.1613
$2^{27}-1$	7.73.262657	2^{27}	134217728	$2^{27}+1$	3^4.19.87211
		2^{28}	268435456	$2^{28}+1$	17.15790321
$2^{29}-1$	233.1103.2089	2^{29}	536870912	$2^{29}+1$	3.59.3033169
		2^{30}	1073741824	$2^{30}+1$	5^2.13.41.61.1321
$2^{31}-1$	2147483647	2^{31}	2147483648	$2^{31}+1$	3.715827883
		2^{32}	4294967296	$2^{32}+1$	641.6700417

TABLEAU DES FACTEURS PREMIERS DE LA SERIE RECURENTE DE FERMAT.

(*Suite.*)

U_n	Diviseurs de U_n		Valeurs de 2^n	V_n	Diviseurs de V_n
$2^{33}-1$	7.23.89.599479	2^{33}	8589934592	$2^{33}+1$	3^3.67.683.20857
		2^{34}	17179869184	$2^{34}+1$	5.137.953.26313
$2^{35}-1$	31.71.127.122921	2^{35}	34359738368	$2^{35}+1$	3.11.43.281.86171
		2^{36}	68719476736	$2^{36}+1$	17.241.433.38737
$2^{37}-1$	223.616318177	2^{37}	137438953472	$2^{37}+1$	3.1777.25781083
		2^{38}	274877906944	$2^{38}+1$	5.229.457.525313
$2^{39}-1$	7.79.8191.121369	2^{39}	549755813888	$2^{39}+1$	3^2.2731.22366891
		2^{40}	1099511627776	$2^{40}+1$	257.4278255361
$2^{41}-1$	13367.164511353	2^{41}	2199023255552	$2^{41}+1$	3.83.8831418697
		2^{42}	4398046511104	$2^{42}+1$	5.13.29.113.1429.14449
$2^{43}-1$	431.9719.2099863	2^{43}	8796093022208	$2^{43}+1$	3.2932031007403
		2^{44}	17592186044416	$2^{44}+1$	17.353.2931542417
$2^{45}-1$	7.31.73.151.631.23311	2^{45}	35184371088832	$2^{45}+1$	3^2.11.19.331.18837001
		2^{46}	70368744177664	$2^{46}+1$	5.277.1013.1657.30269
$2^{47}-1$	2351.4513.13264529	2^{47}	140737488355328	$2^{47}+1$	3.283.165768537521
		2^{48}	281474976710656	$2^{48}+1$	193.65537.22253377
$2^{49}-1$	127.4432676798593	2^{49}	562949953421312	$2^{49}+1$	3.43.4363953127297
		2^{50}	1125899906842624	$2^{50}+1$	5^2.41.101.8101.268501
$2^{51}-1$	7.103.2143.11119.131071	2^{51}	2251799813685248	$2^{51}+1$	3^2.307.2857.6529 43691
		2^{52}	4503599627370496	$2^{52}+1$	17.858001.308761441
$2^{53}-1$	6361.69431.20394401	2^{53}	9007199254740992	$2^{53}+1$	3.107.28059810762433
		2^{54}	18014398509481984	$2^{54}+1$	5.13.37.109.246241.279073
$2^{55}-1$	23.31.89.881.3191.202961	2^{55}	36028797018963968	$2^{55}+1$	3.11^2.683.2971 48912461
		2^{56}	72057594037927936	$2^{56}+1$	257.5153.54410972897
$2^{57}-1$	7.32377.524287.1212847	2^{57}	144115188075855872	$2^{57}+1$	3^2.571.174763.160465489
		2^{58}	288230376151711744	$2^{58}+1$	5.107367629.536903681
$2^{59}-1$	179951.3203431780337	2^{59}	576460752303423488	$2^{59}+1$	3.2833.37171.1824726041
		2^{60}	1152921504606846976	$2^{60}+1$	17.241.61681.4562284561
$2^{61}-1$	. . . . .	2^{61}	2305843009213693952	$2^{61}+1$	3. . . . .
		2^{62}	4611686018427387904	$2^{62}+1$	5.5581.8681.49477.384773
$2^{63}-1$	72.73.127.337.92737.649657	2^{63}	9223372036854775808	$2^{63}+1$	3^3.19.43.5419.77158673929
		2^{64}	18446744073709551616	$2^{64}+1$	. . . . .

(Sera continué.)

THÉORIE DES FONCTIONS NUMERIQUES SIMPLEMENT PÉRIODIQUES

PAR EDOUARD LUCAS, *Professeur au Lycée Charlemagne, Paris.*

(Voir pag. 240 et suiv.)

SECTION XXIV.

De l'apparition des nombres premiers dans les séries récurrentes de première espèce.

Dans les séries récurrentes de première espèce, a et b désignent deux nombres entiers, positifs et premiers entre eux ; il est d'abord évident que les diviseurs premiers de a et de b, ou de $Q = ab$, ne se trouvent jamais comme facteurs dans la série ; il ne sera pas tenu compte de ces diviseurs dans tout ce qui va suivre. On déduit immédiatement de la première des formules (4), la démonstration du théorème de FERMAT. En effet, on a, en négligeant les multiples de p, supposé premier et impair,

$$2^{p-1}\frac{a^p - b^p}{a-b} \equiv \delta^{p-1}, \text{ (Mod. } p)$$

Multiplions les deux termes de la congruence par $\delta = a - b$, nous obtenons

$$2^{p-1}(a^p - b^p) \equiv (a - b)^p, \text{ (Mod. } p) ;$$

supposons $a - b = 2$, et divisons par 2^{p-1} il vient

$$a^p - b^p \equiv a - b, \text{ (Mod. } p) ;$$

ou, encore

$$a^p - a \equiv b^p - b, \text{ (Mod. } p) ;$$

Ainsi, le reste de la division de a^p – a, par p premier, ne change pas lorsque l'on diminue a de deux unités, et par suite de 2, 4, 6, 8, . unités ; mais pour $a = 0$ ou $a = 1$, ce reste est nul ; donc $a^p - a$ est toujours divisible par le nombre premier p, quelque soit l'entier a. Par suite, si le nombre entier a n'est pas divisible par p, la différence $a^{p-1} - 1$ est divisible par p ; c'est précisément l'énoncé du théorème en question.

En supposant maintenant a et b quelconques, mais non divisibles par p, les différences

$$a^{p-1} - 1 \quad \text{et} \quad b^{p-1} - 1$$

sont divisibles par p ; donc, si $a - b$ n'est pas divisible par p, on a

$$U_{p-1} = \frac{a^{p-1} - b^{p-1}}{a - b} \equiv 0 , \quad \text{(Mod. p)}.$$

Par conséquent, les différents termes des séries récurrentes de première espèce contiennent, en exceptant les diviseurs de $Q = ab$ et de $\delta = a - b$, tous les nombres premiers en facteurs.

Mais, s'il est vrai que p divise U_{p-1} , on peut, dans la plupart des cas, trouver un terme de rang inférieur à $p - 1$, et divisible par p. Désignons par ω le rang *d'arrivée ou d'apparition* du no mbre premier p dans la série des U_n ; il résulte des principes exposés (Section XI), que l'on a, pour k entier et positif,

$$U_{k\omega} \equiv 0 , \ \text{(Mod. } p) ;$$

ainsi, tous les termes divisibles par p ont un rang égal à un multiple quelconque du rang d'apparition.

Il résulte encore des principes exposés (Section XIII), que les termes, dont le rang est un multiple quelconque de $(p - 1)\, p^{\lambda - 1}$, sont divisibles par p^{λ} ; mais il peut exister d'autres termes divisibles par p^{λ}, pou r deux raisons bien différentes ; 1° lorsque le rang d'arrivée ω de p diffère de $p - 1$; 2° lorsque le nombre premier p arrive pour la première fois à une puissance supérieure à la première ; mais, cela connu, il est facile de tenir compte de ces singularités. En général, si m désigne un nombre quelconque premier avec Q, et $\varphi(m)$ *l'indicateur de m*, c'est-à-dire le nombre des entiers inférieurs et premiers à 271, on a la congruence

(135) $$U_{\varphi(m)} \equiv 0 , \ \text{(Mod. } m) ;$$

cette congruence correspond au *théorème de* FERMAT *généralisé* par EULER.

Inversement, si l'on a

$$U_n \equiv 0 , \ \text{(Mod. } m) ;$$

On en déduit

$$n = k\mu ,$$

μ désignant un certain diviseur de $\varphi(m)$, et k un entier positif quelconque.

Les résultats que nous venons d'obtenir conduisent à la forme linéaire des diviseurs premiers de U_n. En effet, si ω désigne toujours le rang d'arrivée de p, on a, puisque U_{p-1} est divisible par p,

$$p - 1 = k_0\omega ,$$

et, par suite

(136) $$p = k_0\omega + 1 .$$

Nous appellerons *diviseurs propres de* U_n tous les facteurs premiers de U_n que l'on ne rencontre pas dans les termes de rang inférieur, et *diviseurs impropres*, les facteurs premiers contenus préalablement dans les termes.de la série. On a alors les deux propositions suivantes :

THEOREME I : *Les diviseurs impropres des termes* U_n *des fonctions simplement périodiques sont des diviseurs propres des termes dont le rang est un diviseur de n.*

THEOREME II : *Les diviseurs propres des termes* U_n *des fonctions périodiques de première espèce appartiennent à la forme linéaire* $kn + 1$.

Enfin, si l'on observe que l'on a trouvé

$$U_{2n} = U_n V_n .$$

on a encore :

THEOREME III : *Les diviseurs propres de* V_n *appartiennent à la forme linéaire* $2kn + 1$.

On déduit encore de ce qui précédé la démonstration du théorème, suivant, qui n'est qu'un cas particulier du théorème de LEJEUNE-DIRICHLET, sur les progressions arithmétiques :

THEOREME IV : *Quel que soit l'entier m, il y a une série indéfinie de nombres premiers de la forme linéaire* $km + 1$.

En effet, il est d'abord évident que, pour une valeur suffisamment grande de n, le terme U_n possédé nécessairement un ou plusieurs diviseurs propres de la forme $kn + 1$. Par conséquent, si l'on fait successivement n égal à

$$m, pm, p^2m, p^3m, \ldots p^\lambda m,$$

p étant premier, les termes correspondants possèdent tous, à partir d'un certain rang, des diviseurs de la forme considérée ; le théorème est donc démontré.

Il résulte encore, du théorème I (Section XX), que ces diviseurs appartiennent en outre aux diviseurs de la forme quadratique $x^2 \pm py^2$, suivant que l'on prend pour p un nombre premier de la forme $4q + 3$, ou de la forme $4q + 1$.

Les théorèmes précédents permettent encore de déterminer les diviseurs des fonctions numériques de première espèce ; nous donnerons d'abord les deux exemples suivants dus à EULER.

EXEMPLE I : Soit, dans la série de FERMAT,

$$U_{64} = 2^{64} - 1 = 18446\ 74407\ 37095\ 51615,$$

on a, d'après les formules précédentes,

$$U_{64} = U_1\ V_1\ V_2\ V_4\ V_5\ V_{16}\ V_{32} ;$$

on a immédiatement les décompositions en facteurs premiers

$$U_1 = 1,\ V_1 = 3,\ V_2 = 5,\ V_4 = 17,\ V_8 = 257,\ V_{16} = 65537\ ;$$

et

$$V_{32} = 42949\ 67297.$$

Les diviseurs de V_{32} appartiennent à la forme linéaire $64k + 1$; en essayant les diviseurs premiers de cette forme

$$193,\ 257,\ 449,\ 577,\ 641,$$

on trouve

$$V_{32} = 641 \times 67\ 00417.^{*}$$

L'essai des diviseurs premiers de même forme

$$641,\ 769,\ 1153,\ 1217,\ 1409,\ 1601,\ 2113,$$

et inférieurs à la racine carrée du second facteur de V_{32}, indique presque immédiatement que $67\ 00417$ est un nombre premier.

FERMAT avait annoncé, mais sans dire qu'il en eût la démonstration, dans une lettre du 18 Octobre 1640, que la formule $2^{2^n} + 1$ donnait toujours des nombres premiers. Cette formule se trouve en défaut, d'après la décomposition précédente, due à EULER, pour $n = 5$.

On sait d'autre part, que GAUSS a démontré que l'on peut diviser la circonférence en $2^{2^n} + 1$ parties égales, lorsque ce nombre est premier, et seulement dans ce cas, par la règle et le compas. Nous indiquerons plus loin une méthode de recherche du mode de composition des nombres de cette forme, basée sur la distribution des nombres premiers dans la série de PELL. Par la méthode que nous venons d'exposer, en supposant que le nombre

$$2^{2^6} + 1 = 18446\ 74407\ 37095\ 51617,$$

soit premier, il faudrait à un seul calculateur, pour le démontrer, tout en profitant de la forme $128k + 1$, imposée aux diviseurs de ce nombre, environ *trois mille ans* de travail assidu.[†] Par notre méthode, il suffit de *trente heures,* pour décider si ce nombre est premier ou composé.

EXEMPLE II : Soit encore, dans la série de FERMAT, le terme

$$U_{31} = 2^{31} - 1 = 21474\ 83647$$

dont le rang 31 est un nombre premier. Les diviseurs de U_{31} sont, sans exception, des diviseurs propres appartenant à la forme linéaire $62k + 1$. Mais, d'autre part (Section VIII, Théorème I), en tenant compte des formes quadratiques de ses diviseurs, ou des formes linéaires correspondantes $8k' \pm 1$, on voit

---

[*] Il est inutile, d'après la loi de répétition, d'essayer 257 qui se trouve dans V_8. Nous avons démontré que les diviseurs de V_{32} appartiennent à la forme $128k + 1$. (*Académie de Turin*, janvier 1878)

[†] *Aux mathématiciens de toules les parties du monde. — Communication sur la décomposition des nombres en leurs facteurs simples.* Par M. F. LANDRY. Paris, 1867. (Note de la page 8.)

que tout diviseur premier de U_{31} appartient nécessairement à l'une des formes linéaires

$$248k + 1, \quad 248k + 63.$$

« Or, EULER[*] nous apprend qu'après avoir essayé tous les nombres premiers contenus dans ces deux formes, jusqu'à 46339, racine du nombre $2^{31} - 1$, il n'en a trouvé aucun qui fut diviseur de ce nombre ; d'où il faut conclure conformément à une assertion de FERMAT, 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, Théorie des Nombres, 3e édition, t. I, pag. 229. Paris, 1830.)

EXEMPLE III : On connaissait, depuis quelques années, un nombre premier plus grand que le précédent, indiqué par PLANA, dans son *Mémoire sur la Théorie des Nombres,* du 2 0 Novembre 1859[†]. Soit, en effet

$$V_{29} = 3^{29} + 1 ;$$

ce nombre a tous ses diviseurs propres de la forme $58k + 1$; mais d'autre part, ces diviseurs appartiennent à la forme quadratique $x^2 + 3y^2$, et, par suite, aux formes linéaires $12k + 1$ et $12k + 7$. En combinant l'une de ces formes avec la précédente, on trouve que les diviseurs de V_{29} sont de l'une des deux formes

$$348k + 1, \quad \text{ou} \quad 348k + 175.$$

PLANA a ainsi trouvé la décomposition

$$V_{29} = 2^2 \times 6091 \times 28168\ 76431,$$

et vérifié que le dernier facteur est premier. Il a encore indiqué (*loc. cit.*, pag. 140 et 141) que le quotient

$$\frac{3^{29}-1}{2\times 59} = 58\,16133\,76431,$$

n'a pas de diviseur premier inférieur à 52259, et que le nombre $2^{53} - 1$ n'a pas de diviseur inférieur à 50033. Ces trois assertions sont inexactes ; on a

$$3^{29} - 1 = 2 \times 59 \times 28537 \times 203\ 81027,$$

$$3^{29} + 1 = 22 \times 523 \times 6091 \times 53\ 85997$$

$$2^{53} - 1 = 6361 \times 69431 \times 203\ 94401.$$

Nous ajouterons que l'on trouve encore dans la mémoire de PLANA, la décomposition

$$2^{41} - 1 = 13367 \times 1645\ 11353.$$

---

[*] *Lettre à Bernoulli*, en 1771, — *Mémoires de l'Académie de Berlin*, année 1772, pag. 36.

[†] *Memorie della Reale Accademia delle Scienze di Torino*, 2e série, t. XXI p. 139. Turin, 1863.

EXEMPLE IV : Nous donnerons encore quelques exemples de décomposition de la fonction numérique

$$(2m)^{2m} - 1 ,$$

qui joue un rôle assez important dans les congruences de degré supérieur. Nous avons trouvé les résultats suivants :

$$\begin{cases} 14^7 - 1 = 13 \times 81\,08731, \\ 14^7 + 1 = 3 \times 5 \times 70\,27567, \\ 20^{10} - 1 = 3 \times 7 \times 11 \times 19 \times 61 \times 251 \times 1\,52381, \\ 20^{10} + 1 = 41 \times 401 \times 2801 \times 2\,22361, \\ 22^{11} - 1 = 3 \times 7 \times 67 \times 353 \times 11764\,69537, \\ 22^{11} + 1 = 23 \times 89 \times 28\,54510\,51007, \\ 24^{12} - 1 = 5^2 \times 7 \times 13 \times 23 \times 73 \times 79 \times 349 \times 577 \times 601, \\ 24^{12} + 1 = 97 \times 3\,31777 \times 11347\,93633, \\ 28^{14} - 1 = 3^3 \times 29 \times 113 \times 13007 \times 35771 \times 44\,22461 \\ 30^{15} - 1 = 7^2 \times 19 \times 29 \times 12211 \times 8\,37931 \times 519\,41161 \\ 30^{15} + 1 = 11 \times 13 \times 31 \times 67 \times 271 \times 4831 \times 71261 \times 5\,178311, \end{cases}$$

dont nous donnerons plus tard l'application à de nouvelles recherches sur le dernier théorème de FERMAT.

SECTION XXV.

De l'appparition des nombres premiers dans les séries récurrentes de seconde et de troisième espèce.

En désignant toujours par p un nombre premier quelconque, on sait que le reste de la division de $\Delta^{\frac{p-1}{2}}$ par p est toujours égal à 0, à + 1, ou à – 1, suivant que Δ est un multiple, un résidu quadratique, ou un non-résidu quadratique de p. Nous considérerons les cinq cas suivants.

PREMIER CAS. *p est un diviseur de P.*

On a $U_2 = P$, et par conséquent tous les termes U_n de rang pair de la série sont divisibles par p ; en désignant par p^λ la plus haute puissance de p qui divise P, les rangs des termes divisibles par $p^{\lambda+\mu}$ seront tous les multiples de $2p^\mu$.

DEUXIEME CAS. *p est un diviseur de Q.*

Nous avons, par définition,

$$2^n\sqrt{\Delta}U_n = (P+\sqrt{\Delta})^n - (P-\sqrt{\Delta})^n \ ,$$
$$2^nV_n = (P+\sqrt{\Delta})^n - (P-\sqrt{\Delta})^n \ ;$$

on a donc, en supprimant les multiples de Q, par le remplacement de Δ par P^2, les congruences

$$2^nPU_n \equiv (P+P)^n \ , \quad (\text{Mod. } Q),$$
$$2^nV_n \equiv (P+P)^n \ , \quad (\text{Mod. } Q),$$

ou, plus simplement,

$$U_n \equiv P^{n-1} \ , \quad V_n \equiv P^n \ , \quad (\text{Mod. } Q). \tag{137}$$

Par conséquent, U_n *et* V_n ne sont jamais divisibles par Q ou par l'un de ses diviseurs, puisque P et Q ont été supposés premiers entre eux. D'ailleurs ce résultat s'applique aux séries de première et de troisième espèce ; lorsque l'on a $Q = \pm 1$, comme dans les séries de PELL et de FIBONACCI, nous n'aurons pas à tenir compte du théorème précédent.

TROISIEME CAS. *p est un diviseur de* Δ.

Lorsque p est un nombre premier diviseur de Δ, les formules (4) donnent immédiatement,

$$U_p \equiv 0 \ , \quad V_p \equiv P \ , \quad (\text{Mod. } p). \tag{138}$$

et, par suite cette proposition :

THEOREME : *Dans la série U de seconde espèce, tout diviseur premier p du déterminant* Δ *est un diviseur de* U_p.

Il résulte d'ailleurs des principes exposés précédemment, qu'un diviseur premier impair p de Δ arrive pour la première fois, dans U_p et à *la première puissance.*

QUATRIEME CAS. Δ *est résidu quadratique de p.*

En changeant, dans la première des formules (4), p en $p-1$, on a

$$2^{p-2}U_{p-1} = \frac{p-1}{1}P^{p-2} \frac{(p-1)(p-2)(p-3)}{1.2.3}P^{p-4}\Delta + \ldots . + \frac{p-1}{1}P\Delta^{\frac{p-3}{2}} \ ;$$

et, en appliquant les résultats obtenus (Section XXI) pour les congruences du triangle arithmétique,on a

$$2^{p-2}U_{p-1} \equiv -\left[P^{p-2} + P^{p-4}\Delta + P^{p-6}\Delta^2 + \ldots + P\Delta^{\frac{p-3}{2}}\right], \quad (\text{Mod. } p),$$

et, par suite

$$2^{p-2}U_{p-1} \equiv -P\frac{P^{p-1} - \Delta^{\frac{p-1}{2}}}{P^2 - \Delta}, \quad (\text{Mod. } p).$$

Mais on a, par le théorème de FERMAT, P^{p-1}, (Mod. p), et, puisque Δ est résidu quadratique de p, il en résulte que U_{p-1}, est divisible par p. On a donc cette proposition, qui s'applique aux séries de troisième espèce, en tenant compte du signe de Δ :

THEOREME : *Dans la série récurrente U de seconde ou de troisième espèce, tout nombre premier p, qui admet* Δ *pour résidu quadratique, divise le terme* U_{p-1}.

La seconde des formules (4) donne

$$2^{p-2}V_{p-1} = P^{p-1} + \frac{(p-1)(p-2)}{1.2}P^{p-3}\Delta + \ldots. + \Delta^{\frac{p-1}{2}},$$

et, par suite

$$2^{p-2}V_{p-1} \equiv P^{p-1} + P^{p-3}\Delta + \ldots. + \Delta^{\frac{p-1}{2}}, \quad (\text{Mod. } p),$$

ou bien

$$2^{p-2}V_{p-1} \equiv \frac{P^{p+1} - \Delta^{\frac{p+1}{2}}}{P^2 - \Delta}, \quad (\text{Mod. } p),$$

Mais on a, dans le cas présent

$$P^{p+1} \equiv P^2 \quad \text{et} \quad \Delta^{\frac{p+1}{2}} \equiv \Delta, \quad (\text{Mod. } p);$$

donc

$$2^{p-2}V_{p-1} \equiv 1, \quad (\text{Mod. } p),$$

et finalement, en multipliant par 2 et appliquant le théorème de FERMAT :

(139) $$V_{p-1} \equiv 2, (\text{Mod. } p).$$

CINQUIEME CAS. Δ *est non-résidu quadratique de p.*

On a, comme précédemment,

$$2^p U_{p+1} = \frac{p+1}{1}P^p + \frac{(p+1)p(p-1)}{1.2.3}P^{p-2}\Delta + \ldots.. + \frac{p+1}{1}P\Delta^{\frac{p-1}{2}},$$

$$2^p V_{p+1} = P^{p+1} + \frac{(p+1)p}{1.2}P^{p-1}\Delta + \ldots.. + \Delta^{\frac{p+1}{2}},$$

et, puisque p est premier,

$$2U_{p+1} \equiv P(1 + \Delta^{\frac{p-1}{2}}),$$

$$2V_{p+1} \equiv P^2 + \Delta.\Delta^{\frac{p-1}{2}}.$$

Mais, par hypothèse Δ est non-résidu quadratique de p, et, par suite

$$\Delta^{\frac{p-1}{2}} \equiv -1, \quad (\text{Mod. } p);$$

on a donc

(140) $$U_{p+1} \equiv 0 , \quad V_{p-1} \equiv 2Q, \quad (\text{Mod. } p) ;$$

de là, cette proposition :

THEOREME : *Dans les séries récurrentes U_n de seconde et de troisième espèce, tout,nombre premier p, dont Δ est un non-résidu quadratique, divise U_{p+1} .*

Désignons encore par ω le rang d'arrivée du nombre premier p dans la série des U_n, et par k un nombre entier quelconque ; on a

$$U_{k\omega} \equiv 0 , \quad (\text{Mod. } p) ;$$

par conséquent, si p n'est pas diviseur de Q ou de Δ, on a

$$k_0\omega = p \mp 1,$$

en prenant le signe – ou le signe + suivant que Δ est résidu ou non-résidu de p ; on en déduit

$$p = k_0\omega \pm 1,$$

et, par conséquent :

THEOREME : *Dans les séries récurrentes de seconde espèce, les diviseurs propres de U_ω sont de la forme linéaire $p = k\omega \pm 1$, suivant que Δ est résidu ou non-résidu de p.*

En suivant une marche analogue à celle que nous avons suivie dans le paragraphe précédent, on obtient par la considération des diviseurs de $U_p\lambda$, le théorème suivant.

THEOREME : *Il y a une série indéfinie de diviseurs premiers communs aux formes quadratiques $x^2 - Qy^2$ et $x_1^2 - py_1^2$, lorsque p designe un nombre premier de la forme $4q + 1$; et une série indéfinie de diviseurs communs aux deux formes $x^2 - Qy^2$ et $\Delta x_1^2 - py_1^2$, lorsque p désigne un nombre premier de la forme $4q + 3$.*

Nous appliquerons les résultats qui précédent, aux séries de FIBONACCI et de PELL. Pour la première, on a $P = 1$, $Q = -1$, et $\Delta = 5$, d'autre part, on sait,* que le nombre 5 est résidu de tous les nombres premiers qui sont résidus de 5, et non-résidus de tous les nombres preimiers impairs qui sont non-résidus de 5 lui-même. Par conséquent :

Dans la série de FIBONACCI, *tout nombre premier pair, de la forme* $10q \pm 1$, *divise le terme de rang* $p - 1$, *et tout nombre p premier impair de la forme* $10q \pm 3$ *divise le terme de rang* $p + 1$.

D'ailleurs, les nombres 2 et 5 divisent respectivement les termes dont le rang est un multiple de 3 ou de 5.

---

* GAUSS. — *Disquisitiones Arithmeticæ*. Nos. 121, 122 et 123.

Pour la série de PELL, $P = 2$, $Q = -1$, $\Delta = 2^2 \times 2$; d'autre part, on sait que le nombre 2 est résidu de tout nombre qui n'est pas divisible par 4, ni par aucun nombre premier de la forme $8q + 3$ ou $8q + 5$, et non-résidu de tous les autres ; par conséquent :

Dans la série de PELL, *tout nombre premier p de la forme* $8q \pm 1$ *divise* U_{p-1} , *et tout nombre premier p dà la forme* $8q \pm 3$ *divise* U_{p+1}.

Les théorèmes que nous venons de démontrer conduisent à la décomposition des termes des séries récurrentes de seconde et de troisième espèce, en facteurs premiers. On a ainsi, par exemple, dans la série de FIBONACCI :

$$U_{41} = 1655\ 80141 = 2789 \times 59369,$$

$$U_{53} = 5\ 33162\ 91173 = 953 \times 559\ 45741$$

$$U_{59} = 95\ 67220\ 26041 = 353 \times 27102\ 60697.$$

Nous ajouterons une remarque importante dont on retrouve l'origine dans la correspondance de FERMAT, mais seulement pour les séries de première espèce.

Soit encore, par exemple, la série de FIBONACCI ; les nombres premiers p, des formes linéaires $20q + 13$ et $20q + 17$, divisent U_{p+1}, et l'on a

$$p + 1 = 20q + 14 \quad \text{ou} \quad p + 1 = 20q + 18,$$

et aussi

$$U_{20q+14} = U_{10q+7}V_{10q+7}\ , \quad \text{et} \quad U_{20q+18} = U_{10q+9}V_{10q+9}\ ;$$

mais, d'autre part, les diviseurs de V_{2n+1} appartiennent aux formes linéaires $20q + 1, 9, 11, 19$; par conséquent, les nombres premiers de la forme $20q + 13$ ou $20q + 17$ divisent respectivement U_{10q+7} et U_{10q+7} et disparaissent de la série des V_n qui ne contient donc pas tous les nombres premiers. En appliquant ce raisonnement aux séries de FERMAT et de PELL, on en déduit les principes suivants :

Dans la série de FIBONACCI, *les termes* V_n *ne contiennent aucun nombre premier des formes linéaires* $20q + 13,\ 20q + 17$.

Dans la série de FERMAT, *les termes* V_n *ne contiennent aucun nombre premier de la forme* $8q + 7$.

Dans la série de PELL, *les termes* V_n *ne contiennent aucun nombre premier de la forme* $8q + 5$.

Nous donnons dans le tableau de la page 299, la décomposition en facteurs premiers des termes de la série de FIBONACCI, limitée aux soixante premiers termes.

TABLEAU DES FACTEURS PREMIERS DE LA SERIE RECURENTE DE LEONARD DE PISE.

n	u_n	Div. impropres	Div. propres	n	u_n	Diviseurs impropres	Diviseurs propres
1	1	—	1.	31	13 46269	—	557 × 2417.
2	1	—	1.	32	21 78309	3 × 7 × 47.	2207.
3	2	—	2.	33	35 24578	2 × 89.	19801.
4	3	—	3.	34	57 02887	1597.	3571.
5	5	—	5.	35	92 27465	5 × 13.	1 41961.
6	8	2^3.	—	36	149 30352	$2^4 \times 3^3 \times 17 \times 19$.	107.
7	13	—	13.	37	241 57817	—	73 × 149 × 2221.
8	21	3.	7.	38	390 88169	37 × 113.	9349.
9	34	2.	17.	39	632 45986	2 × 233.	1 35721.
10	55	5.	11.	40	1023 34155	3 × 5 × 7 × 11 × 41.	2161.
11	89	—	89.	41	1655 80141	—	2789 × 59369.
12	144	$2^4 \times 3^2$	—	42	2679 14296	$2^3 \times 13 \times 29 \times 421$.	211.
13	233	—	233.	43	4334 94437	—	4334 94437.
14	377	13.	29.	44	7014 08733	3 × 89 × 199.	43 × 307.
15	610	2 × 5.	61.	45	11349 03170	2 × 5 × 17 × 61.	1 09441.
16	987	3 × 7.	47.	46	18363 11903	28657.	139 × 461.
17	1597	—	1597.	47	29712 15073	—	29712 15073.
18	2584	$2^3 \times 17$.	19.	48	48075 26976	$2^6 \times 3^2 \times 7 \times 23 \times 47$.	1103.
19	4181	—	37 × 113.	49	77787 42049	13.	97 × 61 68709.
20	6765	3 × 5 × 11.	41.	50	1 25862 69025	$5^2 \times 11 \times 3001$.	101 × 151.
21	10946	2 × 13.	421.	51	2 03650 11074	2 × 1597.	63 76021
22	17711	89.	199.	52	3 29512 80099	3 × 233 × 521.	90481.
23	28657	—	28657.	53	5 33162 91173	—	953 × 559 45741.
24	46368	$2^4 \times 3^2 \times 7$.	23.	54	8 62675 71272	$2^3 \times 17 \times 19 \times 53 \times 109$.	5779.
25	75025	5^2.	3001.	55	13 95838 62445	5 × 89.	661 × 4 74541.
26	1 21393	233.	521.	56	22 58514 33717	$3 \times 7^2 \times 13 \times 29 \times 281$.	14503.
27	1 96418	2 × 17.	53 × 109.	57	36 54352 96162	2 × 37 × 113.	43 71901.
28	3 17811	3 × 13 × 29.	281.	58	59 12867 29879	5 14229.	59 × 19489.
29	5 14229	—	5 14229.	59	95 67220 26041	—	353 × 27102 60697.
30	8 32040	$2^3 \times 5 \times 11 \times 61$.	31.	60	154 80087 55920	$2^4 \times 3^2 \times 5 \times 11 \times 31 \times 41 \times 61$.	2521

SECTION XXVI.

Sur la périodicité des fonctions numériques et sur la généralisation du CANON ARITHMETICUS.

Les résultats développés dans les deux sections précédentes, conduisent immédiatement à la périodicité numérique des fonctions que nous étudions ici, par la considération de leurs résidus suivant un module premier p ou suivant un module quelconque m. Cette question a été présentée sous une forme différente, et seulement pour les séries de première espèce, par GAUSS, dans les *Disquisitiones Arithmeticæ,* sous le nom de *théorie des indices,* et développée par JACOBI dans le *Canon Arithmeticus.* Tous ces résultats peuvent être résumés et généralisés, dans le théorème fondamental suivant, qui contient une extension du *Théorème de* FERMAT *généralisé* par EULER.

THEOREME FONDAMENTAL : *Si l'on désigne par* m *un nombre premier avec le produit des racines d'une équation du second degré à coefficients commensurables,*

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

par Δ le discriminant de l'équation, et par $\left(\frac{\Delta}{p}\right)$ le reste de la division de $\Delta^{\frac{p-1}{2}}$ par p, *et égal à* + 1 *ou à* – 1, *suivant que* Δ *est résidu quadratique, ou non-résidu quadratique de p ; et, soit, de plus*

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

on a la congruence

$$U_{\psi(m)} \equiv 0, \quad (\text{Mod. } m). \tag{142}$$

Réciproquement, si U_n *est divisible par* m, *le nombre* 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 ; on retrouve le théorème d' EULER, en supposant $b = 1$.

Quant à la périodicité numérique des résidus, elle résulte des formules d'addition. On a d'abord, en faisant $n = k\omega$ dans les formules (49),

$$2U_{m+k\omega} = U_m V_{k\omega} + U_{k\omega} V_m ,$$

$$2V_{m+k\omega} = V_m V_{k\omega} + \Delta U_m U_{k\omega} ;$$

par conséquent, si ω désigne le rang d'arrivée du nombre premier p dans la série des U_n, on a

$$\left.\begin{aligned} 2U_{m+k\omega} &\equiv V_{k\omega} U_m , \\ 2V_{m+k\omega} &\equiv V_{k\omega} V_m , \end{aligned}\right\} \quad (\text{Mod. } p). \tag{143}$$

Supposons d'abord qu'il s'agisse des fonctions de première espèce, ou lorsque Δ est résidu de p, des fonctions de deuxième et de troisième espèce ; déterminons le nombre k de telle sorte que l'on ait

$$V_{k\omega} \equiv 2, \quad (\text{Mod. } p),$$

ce qui a lieu pour $k\omega = p - 1$, mais aussi, dans la plupart des cas, pour un certain diviseur π de $p - 1$; on aura alors, pour h entier et positif, mais quelconque, les formules

$$\left.\begin{aligned} U_{m+k\omega} &\equiv U_m, \\ V_{m+k\omega} &\equiv V_m, \end{aligned}\right\} \quad (\text{Mod. } p). \tag{144}$$

Celles ci sont analogues aux formules qui donnent la périodicité des fonctions circulaires ; leur application conduit, lorsque l'on remplace le nombre premier p par un module quelconque m, et que l'on tient compte de la *loi de répétition*, à des formules nouvelles contenant la généralisation de résultats indiqués par ARNDT et SANCERY.*

Mais dans le cas des séries de seconde et de troisième espèce il n'en est plus absolument de même, lorsque Δ est non-résidu de p. En posant $\omega' = p + 1$, on a alors ;

$$\left.\begin{aligned} U_{m+\omega'} &\equiv QU_m, \\ V_{m+\omega'} &\equiv QV_m, \end{aligned}\right\} \quad (\text{Mod. } p),$$

et, plus généralement, pour k entier et positif,

$$\left.\begin{aligned} U_{m+k\omega'} &\equiv Q^k U_m, \\ V_{m+k\omega'} &\equiv Q^k V_m, \end{aligned}\right\} \quad (\text{Mod. } p) ; \tag{145}$$

par conséquent, si μ désigne l'exposant auquel appartient Q suivant le module p, on aura

$$\left.\begin{aligned} U_{m+k\mu\omega'} &\equiv U_m, \\ V_{m+k\mu\omega'} &\equiv V_m, \end{aligned}\right\} \quad (\text{Mod. } p).$$

Ainsi dans ce dernier cas, l'amplitude de la période est égale à $\mu\omega'$.

SECTION XXVII.

Sur l'inversion du théorème de FERMAT et sur la vérification des grands nombres premiers.

On sait que le théorème de WILSON qui consiste, pour p premier, dans la congruence

$$1 . 2 . 3 . \ldots . (p-1) \equiv -1, \quad (\text{Mod. } p),$$

* *Journal de Crelle*, t. xxxi ; pag. 260 et suiv. 1846. — *Bulletin de la Société Mathématique de France*, t. iv, pag. 17 et suiv. Paris, 1876.

s'applique exclusivement aux nombres premiers, et donne, par suite, un procédé théorique, mais illusoire dans la pratique, pour reconnaitre si un nombre donné est premier. Il n'en est pas de même du théorème de FERMAT. En désignant par a un nombre inférieur à p on a

$$a^{p-1} \equiv 1, \quad (\text{Mod. } p);$$

mais ce théorème n'est pas restreint aux nombres premiers, et cette congruence peut être vérifiée pour des modules composés ; ainsi, on a, par exemple,

$$2^{37\times 73-1} \equiv 1, \quad (\text{Mod. } 37\times 73).$$

Cependant, on peut énoncer le théorème suivant que l'on doit considérer comme la proposition réciproque de celle de FERMAT.

THEOREME : *Si* $a^x - 1$ *est divisible par p, lorsque* $x = p - 1$, *et n'est pas divisible par p, pour x inférieur à* $p - 1$, *le nombre p est premier.*

On sait que, dans ce cas, a est une *racine primitive de p* ; de plus, il est facile de voir que si $p - 1$ est égal à une puissance de puissance de 2, a est non-résidu quadratique de p. Ce théorème rentre dans le suivant, dont la démonstration résulte immédiatement des propriétés des fonctions numériques simplement périodiques, et s'applique aux trois espèces de séries :

THEOREME FONDAMENTAL : *Si dans l'une des séries récurrentes* U_n , *le terme* 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 ; 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.*

En effet, puisque p divise $U_{p\pm 1}$, tous les termes divisibles par p ont un rang égal à un multiple quelconque d'un certain diviseur de $p \pm 1$; d'autre part, supposons p non premier et égal, par exemple, au produit de deux nombres premiers r et s, on a

$$U_{r\pm 1} \equiv 0, \quad (\text{Mod. } r), \qquad U_{s\pm 1} \equiv 0, \quad (\text{Mod. } s),$$

et, par suite le terme dont le rang est $(r \pm 1)(s \pm 1)$ est divisible par rs ; mais, par hypothèse p divise le terme de rang $rs \pm 1$, et, par conséquent aussi, le terme dont le rang est égal à la différence des précédents, c'est-à-dire

$$(r \pm 1)\,(s \pm 1) - (rs \pm 1)\,,$$

ou bien

$$\pm r \pm s \pm 1 \pm 1\,.$$

Mais ce dernier nombre est évidemment plus petit que rs ; par conséquent, si p n'est pas premier, il divise un terme dont le rang est inférieur à $p \pm 1$; c'est ce que ne suppose pas l'énoncé.

On obtiendrait le même résultat en supposant p égal à un nombre impair

quelconque, en faisant voir (Section XXVI, Théor. fond.) que

$$m \pm 1 - \psi(m)$$

est plus petit que $m \pm 1$.

Dans l'application de ce théorème, on calcule les termes dont le rang est un diviseur quelconque de $p \pm 1$, au moyen des formules d'addition et de multiplication des fonctions numériques, que nous avons exposées ci-dessus. Nous donnerons d'abord un exemple numérique très-simple.

EXEMPLE : Soit

$$2^7 - 1 = 127.$$

Pour savoir si 127 est premier, nous calculons U_{128} dans la série de FIBONACCI ; on a alors les formules

$$V_{4n+2} = V_{2n+1}^2 + 2, \qquad V_{4n} = V_{2n}^2 - 2;$$

on forme ainsi le tableau

$$\begin{aligned}
U_4 &= U_2 (V_1^2 + 2) = U_2 \times 3, \\
U_8 &= U_4 (V_2^2 - 2) = U_4 \times 7, \\
U_{16} &= U_8 (V_4^2 - 2) = U_8 \times 47, \\
U_{32} &= U_{16} (V_8^2 - 2) = U_{16} \times 2207, \\
U_{64} &= U_{32} (V_{16}^2 - 2) = U_{32} \times 48\,70847, \\
U_{128} &= U_{64} (V_{32}^2 - 2) = U_{64} \times 2732\,51504\,97407.
\end{aligned}$$

Or 127 divise le dernier facteur et ne divise aucun des précédents, ainsi 2732 51504 97407 = 127 × 18 68122 08641 , par conséquent 127 est un nombre premier. On simplifie considérablement le calcul par la méthode des congruences, en remplaçant continuellement les nombres V_2, V_4, V_8, ... par leurs résidus suivant le module 127. En tenant compte de cette observation, le tableau précédent devient :

$$\left.\begin{aligned}
V_4 &= 3^2 - 2 = 7, \\
V_8 &= 7^2 - 2 = 47, \\
V_{16} &= 47^2 - 2 \equiv 48, \\
V_{32} &\equiv 48^2 - 2 \equiv 16, \\
V_{64} &\equiv 16^2 - 2 \equiv 0.
\end{aligned}\right\} \quad \text{(Mod. 127).}$$

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, déduite de la

considération des résidus potentiels. Dans celle-ci, on divise le nombre soupçonné premier, par des nombres inférieurs à sa racine carrée, et qui appartiennent à des formes linéaires déterminées que l'on doit d'abord calculer ; *le dividende est constant, et le diviseur variable,* mais inférieur, il est vrai, au nombre essayé ; c'est *l'insuccès* de ces divisions dont le nombre est considérable, malgré la forme linéaire du diviseur, 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, obtenus par la multiplication des fonctions numériques ; ici le *dividende est variable et le diviseur constant ;* par conséquent, on remplace les divisions par de simples soustractions, si l'on a calculé préalablement les dix premiers multiples de ce 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. Ainsi, en cas de réussite, notre méthode est affranchie de l'incertitude des calculs numériques.

Pour vérifier la dernière assertion du P. MERSENNE, sur le nombre supposé premier

$$2^{257} - 1 ,$$

et qui a *soixante-dix-huit* chiffres, il faudrait à l'humanité tout entière, formée de mille millions d'individus, calculant simultanément et sans interruption, un temps supérieur à un nombre de siècles représenté par un nombre de vingt chiffres ; par notre méthode, il suffit d'effectuer successivement les carrés de 250 nombres ayant 78 chiffres, au plus ; cette opération ne demanderait pas, à deux calculateurs habiles contrôlant leurs opérations, plus de huit mois de travail. Nous appliquerons d'abord le théorème fondamental à la vérification des grands nombres premiers de la série de FERMAT qui appartiennent à la forme

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

dans laquelle nous supposerons l'exposant $4q + 3$ égal à un nombre premier tel que $8q + 7$ soit un nombre composé. En effet, si $4q + 3$ n'est pas premier le nombre p est composé ; d'autre part, nous avons démontré (Section XXIII) que si $4q + 3$ et $8q + 7$ sont premiers, le nombre p est encore composé.

En supposant p premier, on a immédiatement

$$A \equiv 2^3 - 1 , \quad (\text{Mod. } 5) ;$$

donc, dans cette hypothèse p est non-résidu de 5, et divise le terme dont rang est égal à $p + 1$ ou à l'un des diviseurs de $p + 1$, dans la série de FIBONACCI ; mais tous ces diviseurs sont de la forme 2^λ, et pour former les termes qui correspondent à ces rangs, il suffit d'appliquer les formules de duplication

des fonctions numériques. On a alors

$$U_{2^{\lambda+1}} = U_{2^\lambda} V_{2^\lambda} \quad et \quad V_{2^{\lambda+1}} = [V_{2^\lambda}]^2 - 2(-1)^{2^\lambda},$$

et l'application du théorème fondamental donne le principe suivant :

THEOREME II : *Soit le nombre* $p = 2^{4q+3} - 1$ *pour lequel* $4q + 3$ *est premier, et* $8q + 7$ *composé ; on forme la série* r_n

$$1,\ 3,\ 7,\ 47,\ 2207, \ldots\ldots$$

par la relation, pour $n > 1$,

$$r_{n+1} = r_n^2 - 2 ;$$

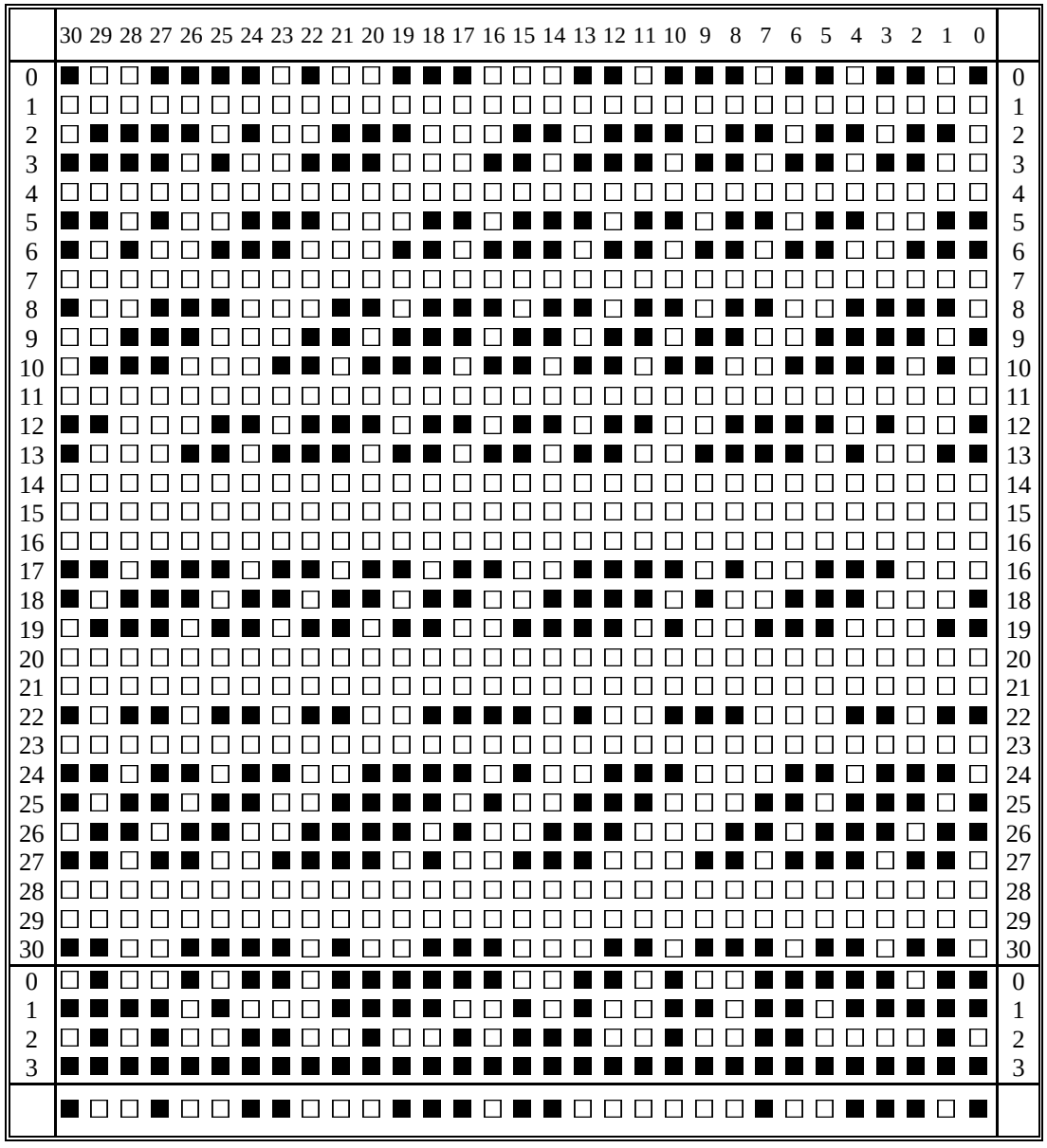
le nombre p est premier lorsque le rang du premier terme, divisible par p, occupe un rang compris entre $2q + 1$ *et* $4q + 2$ *; le nombre p est composé, si aucun des* $4q + 2$ *premiers termes de la série n'est divisible par p ; enfin, si* α *désiqne le rang du premier terme divisible par p, les diviseurs de p appartiennent à la forme linéaire* $2^\alpha K \pm 1$, *combinée avec celles des diviseurs de* $x^2 - 2y^2$.

Dans la pratique, on calcule par congruences, en ne conservant que les résidus suivant le module *p*, ainsi que nous l'avons montré précédemment pour le nombre $p = 2^7 - 1$. Nous avons indiqué un autre procédé de calcul, qui repose sur l'emploi du système de numération binaire, et qui conduira la construction d'un mécanisme propre à la vérification des grands nombres premiers.

Dans ce système de numération, la multiplication consiste simplement dans le 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* ; par conséquent dans l'essai de $2^{31} - 1$, par exemple, il suffira d'opérer sur des nombres ayant, au plus, 31 chiffres. Le tableau de la page 306 donne le calcul du résidu de $V_{2^{26}}$ déduit du résidu de $V_{2^{25}}$ suivant le module $2^{31} - 1$, par la formule

$$V_{2^{26}} \equiv (V_{2^{25}})^2 - 2, \ (Mod.\ 2^{31} - 1) ;$$

les carrés noirs représentent les unités des différents ordres du système binaire, et les carrés blancs représentent les zéros. La première ligne est le résidu de $V_{2^{25}}$; les 31 premières lignes numérotées 0 – 30 figurent le carré de $V_{2^{25}}$; les 4 lignes numérotées 0, 1, 2, 3 du bas de la page indiquent l'addition des unités de chaque colonne, avec les reports ; on a retranché une unité de la première colonne à gauche ; enfin la dernière ligne est le résidu de $V_{2^{26}}$.



CALCUL DU RESIDU DE $V_{2^{26}}$ AU MOYEN DE $V_{2^{25}}$ SUIVANT LE MODULE $2^{31}-1$.

Le tableau de la page 307 contient l'ensemble de tous les résidus de V_2, V_{2^2}, V_{2^3}, ... $V_{2^{29}}$, $V_{2^{30}}$ suivant le module $2^{31}-1$. La dernière ligne, entièrement composée de zéros, nous montre que $2^{31}-1$ est premier.

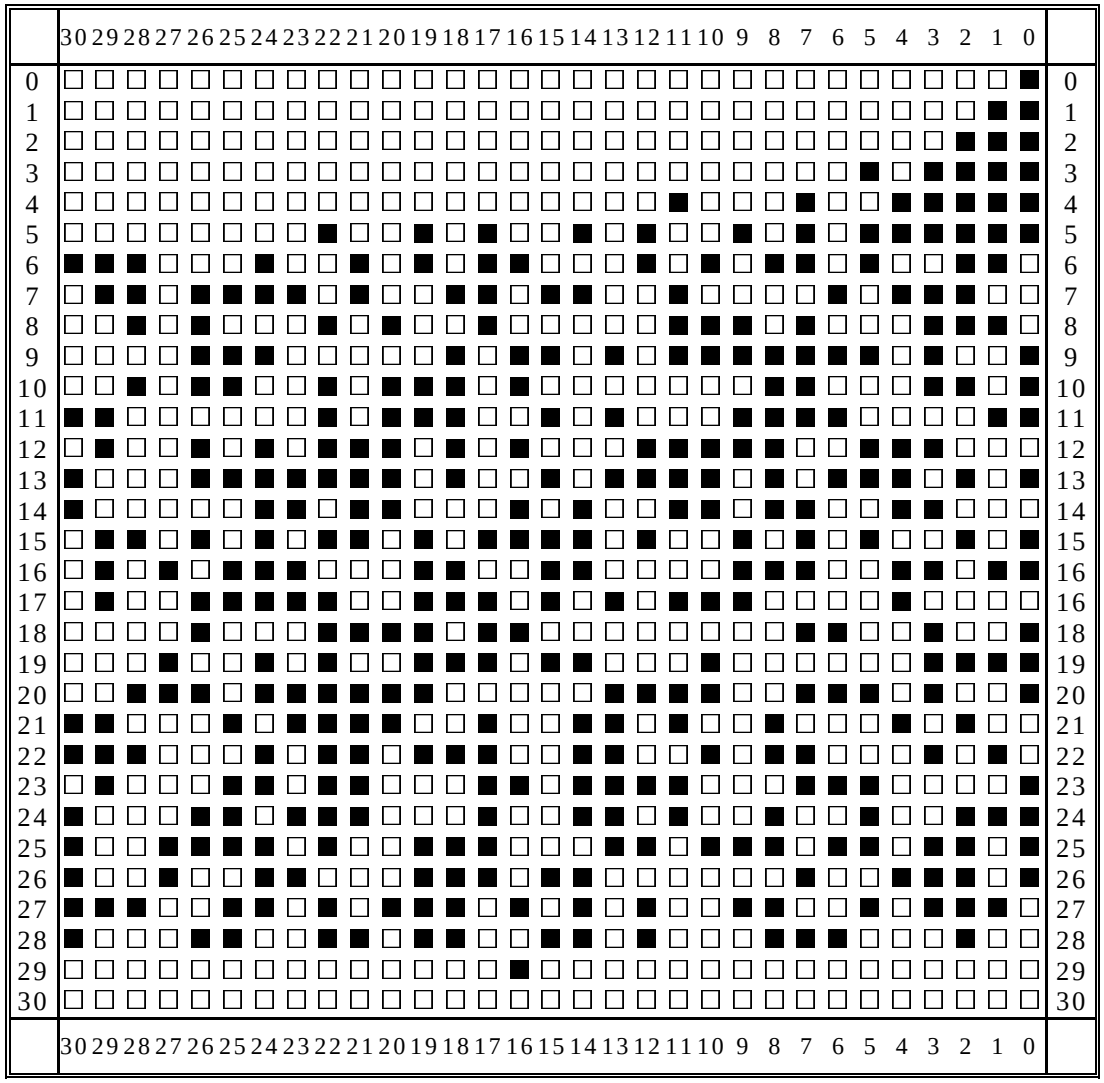


DIAGRAMME DU NOMBRE PREMIER $2^{31}-1$.

Ce tableau est, en quelque sorte, un fragment du *Canon Arithmeticus*, correspondant au nombre premier $2^{31}-1$ pour la racine primitive $\frac{1\pm\sqrt{5}}{2}$.

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 $2^{127}-1$.

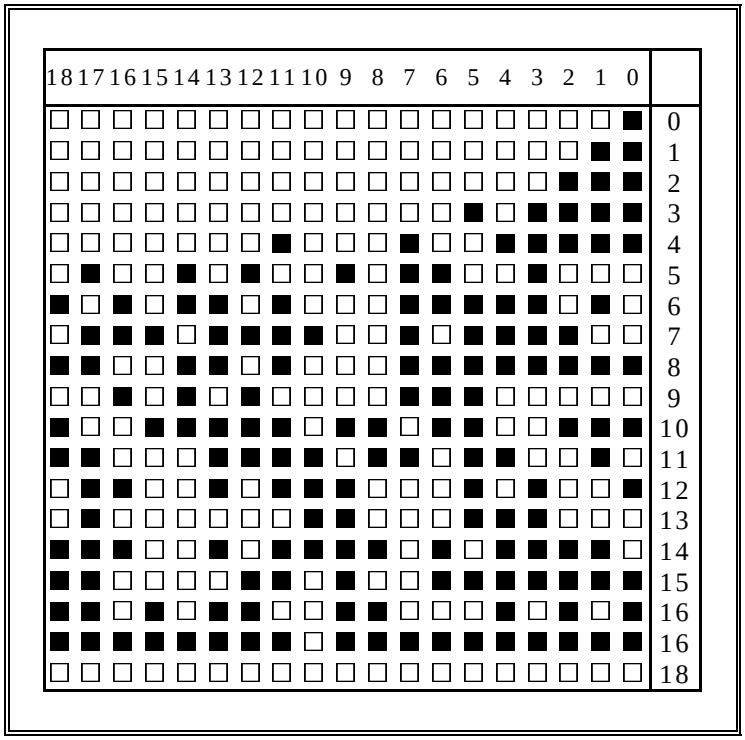


DIAGRAMME DU NOMBRE PREMIER $2^{19} - 1$.

Lorsque l'on aura, par l'application du théorème fondamental, à vérifier de grands nombres premiers de la forme $\frac{3^n \pm 1}{3 \pm 1}$, on emploiera aussi avec succès le système ternaire, dans lequel on se servira seulement des chiffres 0, 1 et $\bar{1}$, à caractéristiques positives on négatives. Pour la vérification des grands nombres de la forme $10^{2^n} + 1$, on se servira facilement du système décimal, pour le calcul des résidus.

Lorsque le nombre essayé n'est pas premier, nous avons vu qu'on ne trouvera aucun résidu nul. Soit, par exemple, le nombre $p = 2^{11} - 1 = 2047$; les résidus que nous considérons sont, dans ce cas,

$$1, 3, 7, 47, 160, 1034, 620, -438, -576, 160, \ldots\ldots,$$

et se reproduisent périodiquement à partir de 160 suivant les cinq résidus

$$160, 1034, 620, -438, -576.$$

On peut donner une autre forme d'énoncé, au Théorème II, et aux suivants, en tenant compte des formules qui concernent les radicaux continus (Section XV) ; on a, par exemple :

THEOREME III : *Pour que le nombres* $p = 2^{4q+3} - 1$ *soit premier, il faut et il suffit que la congruence*

$$3 \equiv 2\cos\frac{\pi}{2^{2q+1}}, \quad (\text{Mod. } p),$$

soit vérifiée, après la disparition successive des radicaux contenus dans la valeur du cosinus.

Nous démontrerons ultérieurement que cette condition est nécessaire et suffisante.

On observera encore que les nombres de la série

$$1, 3, 7, 47, 2207, \ldots\ldots$$

appartiennent tous, à partir du troisième, à la forme linéaire $5q + 2$; mais, d'autre part (Section VIII, Théor. II), les diviseurs de ces nombres appartiennent aux formes linéaires

$$20q + 1, 3, 7, 9 ;$$

par conséquent, chacun des termes de la série précédente contient un diviseur premier de la forme 5q + 2; il en résulte immédiatement cette proposition :

THEOREME IV : *Il y a une infinité de nombres premiers appartenant à la forme linéaire* $5q + 2$.

On voit encore que les nombres de la série ont la forme $8h + 7$; mais, d'autre part, la forme des diviseurs quadratiques indique que les diviseurs de ces nombres sont de l'une des formes $8h + 1$, ou $8h + 7$; par conséquent, chacun des nombres de la série contient au moins un diviseur de la forme 8h + 7, et, par suite :

THEOREME V : *I1 y a une infinité de nombres premiers appartenant à la forme linéaire* $8h + 7$.

Les théorèmes suivants permettent d'arriver à un grand nombre de théorèmes analogues, qui sont des cas particuliers du théorème fondamental de LEJEUNE-DIRICHLET, sur la progression arithmétique. Nous devons observer cependant, que les nombres de la forme $5q + 2$ ne sont pas tous compris dans la série que nous considérons ici, et qu'il en est de même dans tous les autres cas. Ainsi les théorèmes précédents différent, au fond, des cas analogues de la progression arithmétique. La méthode que nous employons s'applique d'ailleurs, très-facilement, a la démonstration du théorème général suivant :

THEOREME VI – *Si A et Q désignent deux nombres quelconques premiers entre eux, la série*

$$r_0, r_1, r_2, r_3, \ldots\ldots r_n ,$$

dans laquelle on a

$$r_0 = A, \quad r_1 = A^2 + 2Q, \quad r_{n+1} = r_n^2 - 2Q^{2^n},$$

contient comme diviseurs, des nombres premiers tous différents.

Les formules de multiplication des fonctions numériques conduisent à des résultats analogues.

Par des considérations semblables aux précédentes, on démontrera les théorèmes suivants.

THEOREME VII : *Soit le nombre* $p = A.2^q - 1$, *et*

$$\left.\begin{array}{ll} 1°, & q \equiv 0, \\ 2°, & q \equiv 1, \\ 3°, & q \equiv 2, \\ 4°, & q \equiv 3, \end{array}\right\} \text{(Mod. 4)}, \quad \text{et} \quad \left.\begin{array}{l} A \equiv 3, \\ A \equiv 7, \\ A \equiv 1, \\ A \equiv 1, \end{array}\right\} \quad \text{ou} \quad \left.\begin{array}{l} \equiv 9, \\ \equiv 9, \\ \equiv 7, \\ \equiv 3, \end{array}\right\} \text{(Mod. 10)} ;$$

on forme les q premiers termes de la série

$$r_1, r_2, r_3, r_4, \ldots ..,$$

par la relation de récurrence $r_{n+1} = r_n^2 - 2,$

en prenant pour r_1 *et* r_2 *les termes* U_A *et* V_A, *de la série de* FIBONACCI. *Le nombre p est premier, lorsque le rang du premier terme divisible par p est égal à q. Si* α *désigne le rang du premier terme divisible par p, les diviseurs de p sont de la forme* $2^\alpha.A.k \pm 1$, *combinée avec celle des diviseurs de* $x^2 - 2y^2$ *et de* $x^2 - 2Ay^2$.

THEOREME VIII *: On obtient un théorème semblable en prenant*

$$p = A.2^q + 1 ,$$

avec les valeurs

$$\left.\begin{array}{ll} 1°, & q \equiv 0, \\ 2°, & q \equiv 1, \\ 3°, & q \equiv 2, \\ 4°, & q \equiv 3, \end{array}\right\} \text{(Mod. 4)}, \quad \text{et} \quad \left.\begin{array}{l} A \equiv 5, \\ A \equiv 5, \\ A \equiv 5, \\ A \equiv 5, \end{array}\right\} \quad \text{ou} \quad \left.\begin{array}{l} \equiv 3, \\ \equiv 9, \\ \equiv 7, \\ \equiv 1, \end{array}\right\} \text{(Mod. 10)} ;$$

soit, par exemple, $p = 3.2^{11} - 1 = 6143$. On forme la série des résidus

4, 18, 322, – 749, 1986, 388, 3110, 3016, 4614, 499, 0 ;

donc, $p = 6143$ est premier.

THEOREME IX : *Soit le nombre*

$$p = A.3^q - 1 ,$$

avec les valeurs

$$\left.\begin{array}{ll} 1°, & q \equiv 0, \\ 2°, & q \equiv 1, \\ 3°, & q \equiv 2, \\ 4°, & q \equiv 3, \end{array}\right\} \text{(Mod. 4)}, \quad \text{et} \quad \left.\begin{array}{l} A \equiv 4, \\ A \equiv 6, \\ A \equiv 2, \\ A \equiv 2, \end{array}\right\} \quad \text{ou} \quad \left.\begin{array}{l} \equiv 8, \\ \equiv 8, \\ \equiv 6, \\ \equiv 4, \end{array}\right\} \text{(Mod. 10)} ;$$

on forme les q premiers termes de la série

$$r_1, r_2, r_3, \ldots,$$

par la formule de récurrence

$$r_{n+1} = r_n^3 + 3r_n^2 - 3,$$

déduite des formules de triplication, avec les conditions initiales

$$r_0 = U_A, \quad r_1 = \frac{U_{3A}}{U_A},$$

dans la série de FIBONACCI ; *le nombre p est premier lorsque le rang du premier terme divisible par p est égal à q ; si α désigne le rang du premier terme divisible par p, les diviseurs de p sont de la forme* $3^\alpha.A.k \pm 1$, *combinée avec celle des diviseurs quadratiques correspondants.*

EXEMPLE : Pour $p = 2.3^7 - 1$, les résidus sont

$$2, 17, 1404, 0 ;$$

donc $p = 4373$ est un nombre premier, puisqu'il n'a pas de diviseur inférieur a sa racine carrée.

THEOREME X : *On a un théorème analogue en supposant*

$$p = A.3^q + 1 ,$$

avec les valeurs

$$\left.\begin{array}{l} q \equiv 0, \\ q \equiv 1, \\ q \equiv 2, \\ q \equiv 3, \end{array}\right\} (\text{Mod. } 4), \quad \text{et} \quad \left.\begin{array}{l} A \equiv 0, \\ A \equiv 0, \\ A \equiv 0, \\ A \equiv 0, \end{array}\right\} \quad \text{ou} \quad \left.\begin{array}{l} \equiv 8, \\ \equiv 6, \\ \equiv 2, \\ \equiv 4, \end{array}\right\} (\text{Mod. } 10) ;$$

et la relation de récurrence

$$r_{n+1} = r_n^3 - 3r_n^2 + 3$$

EXEMPLE : Pour $p = 2.3^6 + 1$, on a les résidus

$$4, 19, -57, 569, -212, 0 ;$$

donc $p = 1459$ est premier.

THEOREME XI : *Soit le nombre*

$$p = 2A.5^q + 1 ,$$

on forme la série limitée à q termes, $r_0, r_1, r_2, r_3, \ldots,$
par la relation de récurrence

$$r_{n+1} = r_n^5 + 5r_n^3 + 5r_n,$$

et les conditions initiales

$$r_0 = U_A , \quad r = U_{5A} ,$$

dans la série de FIBONACCI ; *le nombre p est premier, lorsque le rang du premier terme divisible par p est éqal à q ; il est composé, si aucun des q termes n'est divisible par p ; enfin, si α désigne le rang du premier résidu nul, les diviseurs premiers de p sont de l'une des formes* $2A.5^\alpha k \pm 1$.

SECTION XXVIII.

Sur la division géométrique de la circonférence en parties égales.

Dans la section précédente, nous n'avons considéré que la vérification des nombres premiers par l'emploi de la série de FIBONACCI ; il est clair que toutes les autres séries donnent lieu à de semblables théorèmes ; par suite de l'indétermination laissée à la somme P et au produit Q des deux racines de l'équation fondamentale, on pourra toujours s'assurer du mode de composition d'un nombre p, lorsque l'on connaitra l'une ou l'autre des décompositions de $p + 1$ ou de $p - 1$, en facteurs premiers. Nous donnerons encore l'application du théorème fondamental, aux nombres premiers dans lesquels on peut diviser géométriquement la circonférence, en parties égales.

La théorie de la division géométrique de la circonférence, en parties égales, a été donnée par GAUSS, 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. géométriquement la circonférence en N parties égales, il faut et il suffit que

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

μ étant arbitraire, $a_i . a_j . a_k . . . .$ 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,

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

mais a_5 est divisible par 641 (Section XXVI), et ne peut être compris dans l'expression de N. Il reste donc deux questions importantes à résoudre : 1° comment peut on s'assurer que a_n est premier ? 2° existe-t-il une série indéfinie de nombres premiers a_n ? Nous ne répondrons, pour l'instant, qu'à la première question.

Si a_n est premier, le nombre Q est résidu quadratique de a_n ; donc, dans la série de PELL, V_{a_n-1} est divisible par a_n ; mais $a_n - 1$ a pour diviseurs les nombres,

$$2 , 2^2 , 2^3, ... 2^n ;$$

on a donc, par l'application du théorème fondamental, et par les formules de duplication, le théorème suivant :

THEOREME I : *Soit le nombre* $a_n = 2^{2^n} + 1$ *; on forme la série des* $2^n - 1$ *termes,*

$$6,\ 34,\ 1154,\ 13\ 31714,\ 17\ 73462\ 17794, ... ,$$

tels que chacun d'eux est éqal au carré du précédent diminué de deux unités ; le nombre a_n *est premier, lorsque le premier terme divisible par* a_n *est compris entre les termes de rang* 2^{n-1} *et* $2^n - 1$ *; il est composé, si aucun des ternies de la série n'est divisible par* a_n *; enfin si* $a < 2^n - 1$ *désigne le rang du premier terme divisible par* a_n*, les diviseurs premiers de* a_n *appartiennent à la forme linéaire*

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

On obtiendrait un théorème analogue pour l'essai des grands nombres premiers de la forme

$$A.2^{2^n} + 1 .$$

Le savant P. PEPIN a présenté à l'Académie des Sciences de Paris (*Comptes rendus,* 6 Août 1877), un autre théorème pour reconnaitre les nombres premiers a_n, qui rentre dans notre méthode générale. En effet, au lieu de nous servir de la série de PELL, nous pouvons employer beaucoup d'autres séries récurrentes, et ainsi la série récurrente de première espèce, dont les termes sont donnés par l'expression

$$U_r = \frac{a^r - b^r}{a - b} ,$$

dans laquelle a et b désignent deux nombres entiers arbitraires. En faisant $b = 1$ et a quelconque, on obtiendra un théorème analogue au précédent ; mais si, de plus, par la loi de réciprocité des résidus quadratiques, on choisit pour a un non-résidu de a_n supposé premier, $a = 5$, par exemple, il est clair que le rang du premier résidu nul sera exactement égal à $2^n - 1$. De cette façon, la forme ambigüe donnée à l'énoncé de nos théorèmes disparait, il est vrai, et l'on obtient alors une *condition nécessaire et suffisante* pour que a_n soit premier. Il serait facile de tenir compte de cette observation, et de donner une série de théorèmes analogues, dans la recherche de la condition nécessaire et suffisante pour qu'un nombre $2^n \alpha p \pm 1$ soit premier, lorsque α désigne un produit de facteurs premiers donnés, et p un nombre premier arbitraire. On a, par exemple, les théorèmes suivants.

THEOREME II : *Lorsque* $p = 10q + 7$ *ou* $p = 10q + 9$ *est un nombre premier, le nombre* $2p - 1$ *est premier si l'on a, dans la série de* FIBONACCI,

$$U_p \equiv 0 , \quad (\text{Mod. } 2p-1) ,$$

et réciproquement.

THEOREME III : *Lorsque* $p = 4q + 3$ *est un nombre premier, le nombre* $2p + 1$ *est premier si l'on a, dans la série de* FERMAT,

$$U_p \equiv 0 , \quad (\text{Mod. } 2p+1) ,$$

et réciproquement.

THEOREME IV : *Lorsque* $p = 4q + 3$ *est un nombre premier, le nombre* $2p - 1$ *est premier si l'on a, dans la série de* PELL,

$$U_p \equiv 0 , \quad (\text{Mod. } 2p-1) ,$$

et réciproquement.

On doit cependant observer que si la méthode indiquée par le P. PEPIN, conduit à une forme plus claire et plus précise de l'ènoncé, qui devient ainsi semblable à celui du théorème de WILSON, il est préférable de s'en tenir, dans l'application, à la forme que nous avons adoptée. En effet, l'application de ces théorèmes repose sur une hypothèse, celle de considérer comme premier un nombre pris arbitrairement dans une certaine forme ; il est plus probable de supposer, au contraire, le nombre comme composé, ainsi que semble l'indiquer l'assertion du P. MERSENNE. Par conséquent, au lieu de reculer la vérification, jusqu'à l'extrême limite, par l'emploi des non-résidus quadratiques, il serait plus pratique, dans l'exemple, de se servir de l'un des $\Phi(2^{n-1})$ nombres qui appartiennent à l'exposant 2^{n-1}, pour le module a_n supposé premier ; mais cette recherche directe est fort difficile. On s'assurera cependant que, par le théorème I, il suffit, pour démontrer que a_2, a_3, a_4, sont premiers, d'exécuter respectivement 3, 6, 12, opérations au lieu du nombre 4, 8, 16, qui lui correspond dans l'autre méthode.

SECTION XXIX.

Sur la vérification de l'assertion du P. MERSENNE.

Nous avons indiqué la marche à suivre pour les nombres de la, forme $2^{4q+3} - 1$; il nous reste à indiquer une marche analogue pour les nombres de la forme $p = 2^{4q+1} - 1$, tels que

$$2^{61} - 1 , 2^{97} - 1 , \ldots , 2^{257} - 1.$$

En supposant p premier, -1 est non-résidu de p puisque p est de la forme $4k + 3$, et 2 est résidu de p, puisque p est de la forme $8k + 7$; donc -2 est non-résidu de p. Par conséquent, la série conjuguée de celle de PELL, c'est-à-dire la série provenant de l'équation,

$$x^2 = 2x + 3 ,$$

dans laquelle

$$P = 2 , \quad Q = -3 , \quad \Delta = 2^2 \times (-2) ,$$

est propre à la vérification des nombres premiers que nous considérons, puisque, si p est premier, U_{p+1} est divisible par p. Les diviseurs de $p + 1$ représentent toutes les puissances de 2 jusqu'à l'exposant $4q + 1$; il suffira donc de calculer les résidus de

$$U_1 , \ V_1 , \ V_2 , \ V_4 \ \ldots . \ V_{2^{4q}} ,$$

par les formules ordinaires de duplication.

Mais nous devons encore faire une observation importante, au point de vue du calcul. Puisque l'on emploie la formule

$$V_{2^{\lambda+1}} = (V_{2^{\lambda}})^2 - 2Q^{2^{\lambda}} ,$$

il est bon, si l'on effectue le calcul des résidus dans le système de numération décimale, de supposer $Q = \pm 1$, ou $Q = \pm 10^n$; car sans cela, on double la longueur des calculs, ainsi qu'il est facile de s'en apercevoir ; si l'on opère dans le système de numération binaire, il sera commode de supposer Q égal, en valeur absolue, à l'unité ou à une puissance de 2.

Il est donc préférable d'employer la série récurrente provenant de l'équation

$$x^2 = 4x - 1 ,$$

dans laquelle $a = 2 + \sqrt{3}$, $b = 2 - \sqrt{3}$,

et $p = 4, \quad Q = 1, \quad \Delta = 2^2 \times 3$.

En supposant que $p = 2^{4q+1} - 1$ est un nombre premier, on a, par la loi de réciprocité,

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right),$$

puisque p et 3 sont tous deux des multiples de 4 plus 3 ; d'autre part, par le théorème de FERMAT

$$2^{4q+1} - 1 \equiv 1 , \quad (\text{Mod. } 3) ;$$

donc 3 est non-résidu de p, supposé premier, et, dans ce cas, U_{p+1} est divisible par p. Les diviseurs de $p + 1$ sont égaux à toutes les puissances de 2 jusqu'à $4q + 1$, et, de plus, $Q = 1$.

Par conséquent, on formera la suite des résidus

$$4,\ 14,\ 194,\ 37634,\ \ldots\ .$$

tels que chacun d'eux est égal au carré du précédent diminué de deux unités.

EXEMPLE : Soit le nombre $2^{13} - 1 = 8191$; on trouve les résidus

4, 14, 194, 4870, 3953, 5970, 1857, 36, 1294, 3470, 128, 0 ;

donc le nombre $2^{13} - 1$ est premier.

On a donc le théorème suivant :

THEOREME : *Soit le nombre* $p = 2^{4q+1} - 1$; *on forme la série des résidus*

$$4,\ 14,\ 194,\ 37634,\ \ldots\ ,$$

tels que chacun d'eux est égal au carré du précédent diminué de deux unités ; le nombre p *est composé, si aucun des* $4q + 1$ *premiers résidus n'est égal à 0 ; le nombre* p *est premier si le premier résidu nul occupe un rang compris entre* $2q$ *et* $4q + 1$ *; si le ranq du premier résidu est égal à* $\alpha < 2q$ *, les diviseurs de* p *appartiennent à la forme linéaire*

$$2^{\alpha+1}k + 1.$$

On aurait encore des théorèmes analogues pour les nombres de la forme

$$A \,.\, 2^{4q+1} - 1\ .$$

Avant de terminer ce paragraphe, nous ferons observer que nous pensons n'avoir qu'effleuré le sujet qui nous occupe. Il reste à trouver, comme pour les nombres premiers, un criterium des nombres composés, affranchi de l'incertitude des calculs numériques ; dans un grand nombre de cas, lorsque le nombre essayé n'est pas premier, il se présente une période dans la suite des résidus ; mais, s'il est vrai, comme nous l'avons démontré (Section XXVI), que cette période existe, lorsque l'on considére l'ensemble des résidus de tous les termes de la série récurrente, il n'est pas démontré que cette période se manifestera, si l'on ne considére qu'un certain nombre d'entre eux, dont les rangs sont en progression géométrique. C'est là un problème important à résoudre.

En second lieu, lorsque l'ensemble des calculs démontre que le nombre essayé n'est pas premier, peut-on arriver facilement, par la connaissance de la série des résidus calculés, à la décomposition du nombre que l'on avait supposé premier ? Ces résidus forment, comme nous l'avons dit, un fragment d'un *Canon Arithmeticus généralisé,* que l'on peut comparer aux tables des logarithmes des sinus et des cosinus, ainsi que l'on compare le Canon Arithmeticus lui-même, aux tables des logarithmes des nombres. C'est là un second problème à résoudre.

Nous avons encore indiqué (Sections IX et XXI), une première généralisation de l'idée principale de ce mémoire, dans l'étude des séries récurrentes qui naissent des fonctions symétriques des racines des équations algébriques du troisième et du quatrième degré, et, plus généralement, des racines des équations de degré quelconque, à coefficients commensurables. On trouve en particulier, dans l'étude de la fonction.

$$U_n = \frac{\Delta(a^n, b^n, c^n, \ldots\ldots)}{\Delta(a, b, c, \ldots\ldots)},$$

dans laquelle a, b, c,....désignent les racines de l'équation, et $\Delta(a, b, c, \ldots)$ la *fonction alternée* des racines, ou la racine carrée du discriminant de 1'équation, la généralisation des principales formules contenues dans la première partie de ce travail.

Enfin, il reste à développer la théorie de la division des fonctions numériques, et son application à l'analyse indéterminée du second degré et des degrés supérieurs ; c'est une étude que nous espérons publier prochainement. Nous donnons d'ailleurs, dans le dernier paragraphe qui suit, une autre généralisation des fonctions numériques périodiques, déduite de la considération des séries ordonnées suivant les puissances de la variable.

SECTION XXX.

Sur la périodicité numérique des coefficients différentiels des fonctions rationnelles d'exponentielles.

L'étude des nombres premiers contenus dans les dénominateurs des coefficients des puissances de la variable, dans les développements en séries, lorsque l'on suppose ces coefficients réduits à leur plus simple expression, a conduit EISENSTEIN à la découverte d'un théorème remarquable. En effet, ce théorème fournit un criterium qui permet de décider, à la seule inspection des facteurs premiers du dénominateur, si la fonction qui représente la somme de la série supposée convergente, est *algébrique* ou *transcendante*.

On sait encore que l'étude des facteurs premiers contenus dans les numérateurs des coefficients B_n, de $\frac{z^n}{1.2.3\ldots n}$ dans le développement de $\frac{z}{1-e^z}$, ou, en d'autres termes, dans les numérateurs des *nombres de* BERNOULLI, a conduit CAUCHY, MM. GENOCCHI et KUMMER, à d'importants résultats sur la théorie des résidus quadratiques, et sur celle de l'équation indéterminée

$$x^p + y^p + z^p = 0,$$

dont FERMAT a affirmé l'impossibilité en nombres entiers, pour $p > 2$. Ainsi M. KUMMER a démontré que cette équation ne peut être vérifiée par des nombres entiers, lorsque p ne se trouve pas comme facteur dans les numérateurs des nombres de BERNOULLI $B_2, B_4, B_6, \ldots B_{p-3}$.*

En se plaçant à un point de vue différent, MM. CLAUSEN et STAUDT ont donné pour ces nombres cette expression remarquable

$$B_{2n} = A_{2n} - \frac{1}{2} - \frac{1}{\alpha} - \frac{1}{\beta} - \ldots - \frac{1}{\lambda} ,$$

dans laquelle A_{2n} est un nombre entier, et les dénominateurs $2, \alpha, \beta, \gamma, \ldots . \lambda$, tous les nombres premiers qui surpassent d'une unité tous les diviseurs de $2n$. Cette formule conduit au procédé le plus rapide pour le calcul de ces nombres ; M. ADAMS vient de donner, par son emploi, les valeurs des 62 premiers nombres (*British Association*, — Plymouth, Août 1877.)

Nous avons indiqué aussi comment l'application combinée des théorèmes de FERMAT et de STAUDT conduit à cette propriété que les nombres

$$a\,(a^{2n} - 1)\,B_{2n} ,$$

sont entiers, quel que soit l'entier a. Nous allons montrer que l'étude des coefficients de $\dfrac{x^n}{1.2.3\ldots n}$ dans le développement des fonctions rationnelles d'exponentielles, ou, en d'autres termes, les coefficients différentiels de ces fonctions, pour x = 0, conduit à des propriétés importantes.

On sait, en effet, que si l'on remplace x par les nombres entiers consécutifs dans la fonction

$$\phi(x) = Aa^x + Bb^x + Cc^x + Dd^x + \ldots .$$

dans laquelle $A, B, C, D, \ldots .$ et $a, b, c, d, \ldots .$ sont entiers, on a, pour p premier et k entier quelconque, la congruence

$$\phi\,[x + k(p-1)] \equiv \phi\,(x) \ , \text{(Mod. } p). \tag{148}$$

Nous avons étendu cette propriété aux fonctions numériques U_n et V_n ; il est facile, de voir que cette proposition s'applique aux coefficients différentiels d'une fonction entière de e^x et de e^{-x} . Il nous reste à montrer que cette

*Nous avons modifié les diverses notations qui concernent ces nombres. La présente notation se prête beaucoup plus facilement aux développements que comporte la théorie de ces nombres. Voir, sur ce sujet, les Notes insérées dans les *Comptes rendus de l'Académie des Sciences de Paris* (Septembre 1876), dans les *Annali di Matematica* (2e série, tome VIII), dans les *Nouvelles Annales de Mathématiques* (2e série, tome XVI, pag. 157), dans la *Nouvelle Correspondance Mathématique* (tome II, pag. 328, et tome III, pag. 69), dans *The Messenger of Mathematics*, (Octobre 1877), etc.

proposition s'applique encore aux coefficients différentiels d'une fonction rationnelle de e^x et de e^{-x}.

Soit d'abord

(149) $$\text{séc } x = 1 + a_2x^2 + a_4x^4 + a_6x^6 + \ldots ;$$

M. SYLVESTER a appelé *nombres Eulériens* (*Comptes rendus,* t. LII, pag. 161), les coefficients, pris en valeur absolue, déterminés par la relation

(150) $$E_{2n} = (-1)^n\, 1, 2, 3 \ldots (2n)\, Q_{2n} ;$$

on a, par le changement de x en $x\sqrt{-1}$, la formule symbolique

(151) $$u = \frac{2}{e^x + e^{-x}} = e^{Ex},$$

dans laquelle on remplacera, dans le développement du second membre les exposants de E par des indices ; ainsi

$$\frac{d^n u_0}{dx_0^n} = E_n.$$

En chassant les dénominateurs de l'identité (151), on obtient, par l'identification des coefficients de x^n, la formule

(152) $$(E + 1)^n + (E - 1)^n = 0 ,$$

qui permet de calculer les nombres Eulériens par voie récurrente. On a aussi le déterminant

(153) $$E_{2n} = (-1)^n \begin{vmatrix} 1 & 1 & 0 & 0 & . & . & . & . & 0 \\ 1 & 6 & 1 & 0 & . & . & . & . & 0 \\ 1 & 15 & 15 & 1 & . & . & . & . & 0 \\ . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & 0 \\ 1 & C_{2n}^2 & C_{2n}^4 & C_{2n}^6 & . & . & . & . & C_{2n}^2 \end{vmatrix} ;$$

ce déterminant est formé par les lignes de rang pair et les colonnes de rang impair du triangle arithmétique. Les nombres Eulériens sont entiers et impairs ; SHERK a démontré qu'ils sont terminés alternativement par les chiffres 1 et 5[*]. Ces propriétés sont des cas particuliers des suivantes.

En tenant compte des résultats obtenus (Section XXI), sur les congruences du triangle arithmétique, la formule (152) donne, pour p premier, et $n = p - 1$

(154) $$E_{p-1} + E_{p-3} + E_{p-5} + \ldots + E_2 + E_1 \equiv 0, \quad (\text{Mod. } p);$$

on a donc cette proposition :

[*] *Journal de Crelle,* t. 79, pag. 67.

THEOREME : *Si p est un nombre premier, la somme des nombres Eulériens, pris avec les signes alternés + et −, dont l'indice est plus petit que p, est divisible par p.*

Les premières valeurs de E sont donnés par les relations

$$\begin{aligned} E_2 + E_0 &= 0, \\ E_4 + 6E_2 + E_0 &= 0, \\ E_6 + 15E_4 + 15E_2 + E_0 &= 0, \\ &\cdots\cdots\cdots, \\ &\cdots\cdots\cdots; \end{aligned}$$

on a ensuite, par congruence, à partir de E_{p+1} pour le module premier p

$$\begin{aligned} E_{p+1} + E_0 &\equiv 0, \\ E_{p+3} + 3E_{p+1} + 3E_2 + E_0 &\equiv 0, \\ E_{p+5} + 10E_{p+3} + 5E_{p+1} + 5E_4 + 10E_2 + E_0 &\equiv 0, \\ &\cdots\cdots\cdots\cdots\cdots, \\ &\cdots\cdots\cdots\cdots\cdots; \end{aligned}$$

la comparaison des deux groupes de formules qui précédent, donne successivement

$$\begin{aligned} E_{p+1} &\equiv E_2, \quad (\text{Mod. } p), \\ E_{p+3} &\equiv E_4, \quad " \\ E_{p+5} &\equiv E_6, \quad " \\ &\cdots\cdots\cdots \end{aligned} \tag{155}$$

On obtient de même, en général, pour k entier quelconque

$$E_{2n+k(p-1)} \equiv E_{2n}, \quad (\text{Mod. } p), \tag{156}$$

et, par suite :

THEOREME : *Les résidus des nombres Eulériens, suivant un module premier quelconque, se reproduisent périodiquement dans le même ordre, comme les résidus des puissances des nombres entiers.*

Posons maintenant

$$u^\alpha = \left(\frac{2}{e^x + e^{-x}}\right)^\alpha = E_{\alpha,0} + E_{\alpha,1}\frac{x}{1} + E_{\alpha,2}\frac{x^2}{1.2} + \ldots + E_{\alpha,n}\frac{x^n}{1.2\ldots n} + \ldots$$

ou, sous la forme symbolique

$$u^\alpha = e^{E_\alpha x}, \tag{157}$$

les coefficients $E_{\alpha,n}$ sont déterminés par la relation symbolique

$$E_{\alpha,n} = [E' + E'' + E''' + \ldots + E^{(\alpha)}]^n, \tag{158}$$

dans le développement de laquelle on remplace les exposants de E', E'', ... $E^{(a)}$ par des indices, et en supprimant les accents. On a aussi la formule

(159) $$E_{\alpha,n} = [E_{\alpha-1} + E_1]^n ,$$

dans laquelle en remplace les exposants de $E_{\alpha-1}$ et de E_1, par des seconds indices. Ces nombres $E_{\alpha,n}$ que nous appellerons les *nombres Eulériens d'ordre* α sont entiers pour α entier et positif ; on démontre, comme ci-dessus, que leurs résidus suivant un module premier se reproduisent périodiquement, et que l'on a encore

(160) $$E_{\alpha,n} \equiv E_{\alpha,n+k(p-1)} , \quad (\text{Mod. } p) .$$

Ces considérations s'appliquent, en général, aux coefficients différentiels d'une fraction rationnelle de e^x, mais, dans certaines conditions, comme dans le cas de

$$\frac{\phi(1)}{\phi(e^x)} .$$

Cependant, lorsque $\phi(1)$ est nul, comme dans le développement de $\frac{1}{1-e^x}$ qui contient les nombres de BERNOULLI, ce théorème ne se présente plus immédiatement, puisque les coefficients ne sont plus entiers, et contiennent en dénominateur une série indéfinie de nombres premiers. Alors, on les multiplie par d'autres fonctions telles que

$$a\ (a^n - 1)$$

afin de les rendre entiers, et d'appliquer les résultats qui proviennent des congruences du triangle arithmétique.

PARIS, Décembre, 1877.