REMARQUES

SUR

LA THÉORIE DES NOMBRES

ET SUR LES FRACTIONS CONTINUES

PAR

Eugène CATALAN

ASSOCIÉ DE L'ACADÉMIE

Présenté, à la Classe des sciences, dans la séance du 14 octobre 1893.)

AVERTISSEMENT

On peut voir, dans les *Mélanges mathématiques* (t. III, p. 160), qu'une démonstration du théorème de Bachet, donnée par Legendre, est inexacte (*). Cette erreur de l'illustre Géomètre est loin d'être unique. A la page 213 de la *Théorie des Nombres* (1830, t. I), on lit : « tout diviseur de la somme t^2+u^2, » composée de deux carrés premiers entre eux, est également la somme de » deux carrés, premiers entre eux. »

Legendre prouve bien que le diviseur est la *somme de deux carrés;* mais il oublie de démontrer que ces deux carrés sont *premiers entre eux.* Cet oubli est, pour ainsi dire, fort heureux; car, parmi les décompositions du diviseur, il en existe, parfois, pour lesquelles les deux carrés ont un facteur commun (**).

Si le savant auteur de la *Théorie des Nombres,* de la *Théorie des fonctions*

(*) Elle a été, en 1869, critiquée par Gerono (*Nouvelles Annales*, p. 455).

(**) *Exemple.* Soient

$$t = 11, \quad u = 27.$$

La somme

$$t^2 + u^2 = 121 + 729 = 850 = 2 \times 425.$$

Or,

$$425 = 400 + 25.$$

Il est vrai que ce diviseur 425 est décomposable aussi en

$$361 + 64 = 19^2 + 8^2,$$

conformément à l'énoncé.

elliptiques, etc., s'est trompé en quelques points (*), ses disciples ont, en quelques points aussi, donné des démonstrations qui laissent à désirer (**).

Afin d'épargner, aux jeunes Géomètres, l'ennui de *discuter* les démonstrations contenues dans les livres qu'ils peuvent avoir en mains, j'ai tâché, dans ces derniers temps, de revoir ces démonstrations, et de les rendre exactes et simples.

C'est le résumé de ces recherches que j'ai l'honneur de présenter à l'Académie. Naturellement, il ne contient presque rien de neuf.

(*) En 1858, l'Académie des Sciences proposa, comme sujet de concours, la question suivante :

« *Établir rigoureusement la proposition de Legendre, ..., dans le cas où elle serait exacte,* » *ou, dans le cas contraire, montrer comment on doit la remplacer.* »

L'un des concurrents, M. Athanase Dupré, démontra que le théorème entrevu par Legendre (*Th. des Nombres,* t. II, p. 76) est *faux*. Au moins, la conclusion de ce professeur n'a pas été contestée, à ce que je crois.

(**) Par exemple, dans le *Cours d'Algèbre supérieure,* de SERRET (3e édit., t. I, p. 32), le célèbre professeur démontre le théorème sur les diviseurs d'une somme de deux carrés, théorème dont l'énoncé a été *rectifié;* mais sa rédaction me paraît inintelligible.

Liége, le 21 septembre 1893.

REMARQUES

SUR

LA THÉORIE DES NOMBRES

ET SUR LES FRACTIONS CONTINUES

I

Fractions continues inverses.

1. ***Préliminaires.*** Soient, sous forme abrégée, les fractions continues *inverses* (*) :

$$x = a, b, c, \ldots p, q, r \quad (1)$$

$$y = r, q, p, \ldots c, b, a \text{ (**)} \quad (2)$$

Soient

$$\frac{P}{P'}, \frac{Q}{Q'}, \frac{R}{R'} = x$$

les trois dernières réduites de x.

On a

$$R = Qr + P, \quad Q = Pq + N, \ldots C = Bc + A \text{ (***)} \quad (3)$$

$$R' = Q'r + P', \quad Q' = P'q + N', \ldots C' = B'c + 1 \quad (4)$$

Donc

$$\frac{R}{Q} = r, q, p, \ldots c, b, a = y \quad (5)$$

$$\frac{R'}{Q'} = r, q, p, \ldots c, b \text{ (†)} \quad (6)$$

(*) Gerono, *Nouvelles Annales de Mathématiques*, 1842, p. 1.

(**) Nous supposons, une fois pour toutes, $x > 1$.

(***) $A = a$.

(†) A cause de $B' = b$.

Cette nouvelle fraction continue est le développement de y, abstraction faite du dernier terme a. Autrement dit, $\frac{R'}{Q'}$ est l'avant-dernière réduite de y. On a donc ce théorème important, connu sous le nom de *théorème de Gerono* (*) :

$\frac{Q}{Q'}, \frac{R}{R'}$ *étant les deux dernières réduites de la fraction continue* x, *celles de la fraction inverse,* y, *sont* $\frac{R'}{Q'}, \frac{R}{Q}$.

2. *Remarque.* Soit $\frac{X}{X'}$ la réduite antépénultième de y.

A cause de

$$R = R'a + X, \quad Q = Q'a + X', \quad \ldots\ldots\ldots\ldots \quad (7)$$

on a

$$\frac{X}{X'} = \frac{R - R'a}{Q - Q'a} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (8)$$

3. *Application.* Soient, pour fixer les idées :

$$x = 3, \quad 2, \quad 5, \quad 4, \quad 2;$$

$$y = 2, \quad 4, \quad 5, \quad 2, \quad 3.$$

Les réduites de x sont, d'après la règle ordinaire :

$$\frac{3}{1}, \quad \frac{7}{2}, \quad \frac{38}{11}, \quad \frac{159}{46}, \quad \frac{356}{103};$$

et celles de y :

$$\frac{2}{1}, \quad \frac{9}{4}, \quad \frac{47}{21}, \quad \frac{103}{46}, \quad \frac{356}{159}.$$

On a donc, dans ce cas particulier :

$$Q = 159, \quad Q' = 46, \quad R = 356, \quad R' = 103, \quad X = 47, \quad X' = 21;$$

puis

$$\frac{356}{159} = \frac{R}{Q}, \quad \frac{103}{46} = \frac{R'}{Q'}, \quad \frac{47}{21} = \frac{356 - 103.3}{159 - 46.3};$$

conformément à ce qui précède.

(*) Ne l'ayant trouvé ni dans Lagrange ni dans Legendre, je pense qu'on peut l'attribuer au savant et regretté fondateur des *Nouvelles Annales*.

II

Fonctions continues symétriques.

4. Problème. *Connaissant*

$$x = a, b, c, \ldots, p, q, r, \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (1)$$

$$y = r, q, p, \ldots, c, b, a; \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (2)$$

trouver

$$u = a, b, c, \ldots p, q, r, r, q, p, \ldots c, b, a \ (*) \quad . \quad . \quad . \quad . \quad . \quad . \quad (9)$$

Les formules (3), (4) donnent

$$x = \frac{R}{R'} = \frac{Qr + P}{Q'r + P'} \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (10)$$

Pour obtenir la valeur de u, il suffit de remplacer, dans cette expression de x, r par

$$r + \frac{1}{y} = r + \frac{Q}{R}.$$

Ainsi

$$u = -\frac{Q\left(r + \frac{Q}{R}\right) + P}{Q'\left(r + \frac{Q}{R}\right) + P'} = \frac{R + \frac{Q^2}{R}}{R' + \frac{QQ'}{R}},$$

ou

$$u = \frac{Q^2 + R^2}{QQ' + RR'} \ (**) \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (11)$$

5. *Remarque.* La fraction $\frac{Q^2 + R^2}{QQ' + RR'}$ est *irréductible*. En effet, les nombres entiers Q, Q', R, R' satisfont à la condition

$$QR^2 - RQ' = \pm 1 \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (12)$$

(*) La fraction u est composée d'un nombre *pair* de ternes; ce que l'on peut toujours supposer, d'après une propriété connue.

(**) *Nouvelles Annales*, 1849, p. 177; *Mémoire sur les fractions continues*, p. 137; etc.

6. *Autre remarque.* L'avant-dernière réduite de y étant $\frac{R'}{Q'}$; si, dans la valeur de x (4), on remplace r par $r+\frac{Q'}{R}$, on aura l'avant-dernière réduite de u. On trouve, ainsi, la fraction *irréductible* $\frac{QQ'+RR'}{Q'^2+R'^2}$.

7. *Propriété importante.* Soit, comme ci-dessus,

$$u = a, b, c, \ldots p, q, r, r, q, p, \ldots c, b, a \quad \ldots\ldots\ldots \quad (9)$$

une fraction continue symétrique. On vient de voir que ses deux dernières réduites sont

$$\frac{QQ'+RR'}{Q'^2+R'^2} = \frac{Q_1}{Q'_1}, \quad \frac{Q^2+R^2}{QQ'+RR'} = \frac{R_1}{R'_1} \ (*) \quad \ldots\ldots\ldots \quad (13)$$

Donc

Le numérateur de l'avant-dernière réduite de u *est égal au dénominateur de la dernière;* ou, sous forme abrégée,

$$Q_1 = R'_1. \quad \ldots\ldots\ldots\ldots\ldots \quad (14)$$

8. *Autre propriété.* La réduite $\frac{R_1}{R'_1}$ étant de rang *pair,* on doit, en appliquant l'égalité (12), adopter le signe —. Ainsi

$$Q_1R'_1 - P_1Q'_1 = -1;$$

ou, à cause de la condition (14),

$$Q_1^2 + 1 = R_1Q'_1; \quad \ldots\ldots\ldots\ldots \quad (15)$$

ou enfin

$$(QQ'+RR')^2 + 1 = (Q^2+R^2)(Q'^2+R'^2) \quad \ldots\ldots\ldots \quad (16)$$

Cette égalité nous servira plus loin (**).

(*) J'emploie les notations Q_1, Q'_1, R_1, R'_1, pour simplifier.

(**) On peut encore la démontrer en observant que

$$1 = (QR' - RQ')^2 \quad \ldots\ldots\ldots\ldots \quad (12)$$

9. *Application.* Soit

$$u = 1, 2, 3, 5, 2, 1.$$

Les réduites successives sont

$$\frac{2}{1}, \quad \frac{3}{2}, \quad \frac{10}{7}, \quad \frac{33}{23}, \quad \frac{76}{53}, \quad \frac{105}{76}.$$

Avec les notations précédentes, on a donc :

$$Q = 3, \quad Q' = 2, \quad R = 10, \quad R' = 7, \quad Q_1 = 76, \quad Q'_1 = 53, \quad R_1 = 109, \quad R'_1 = 76 = Q_1.$$

On doit trouver :

$$76 = 3.2 + 10.7, \quad 53 = 2^2 + 7^2, \quad 109 = 3^2 + 10^2;$$

ce qui a lieu, en effet.

10. Problème. *Trouver une fraction* u *dont le développement soit symétrique.*

Prenons, arbitrairement, $Q = 37$, $R = 42$: ces deux nombres sont premiers entre eux. Il en résulte

$$R_1 = 37^2 + 42^2 = 1\,369 + 1\,764 = 3\,133;$$

puis l'équation

$$37R' - 42Q' = -1 \ (*)$$

Celle-ci est vérifiée par $Q' = 15$, $R' = 17$.

D'après ces valeurs de Q, Q', R, R' :

$$Q_1 = QQ' + RR' = 37.15 + 42.17 = 555 + 714 = 1\,269,$$

$$Q'_1 = Q'^2 + R'^2 = 15^2 + 17^2 = 225 + 289 = 514.$$

La fraction demandée est donc $\frac{3\,133}{1\,269}$.

(*) Pour le motif qui sera indiqué tout à l'heure, j'adopte le signe —.

En effet, on trouve

$$u = 2, 2, 7, 1, 1, 7, 2, 2;$$

puis les réduites

$$\frac{2}{1}, \frac{5}{2}, \frac{37}{15}, \frac{42}{17}, \frac{79}{32}, \frac{595}{241}, \frac{1\,269}{514}, \frac{3\,155}{1\,269}.$$

La *condition de possibilité* est donc qu'une des équations

$$QR' - RQ' = \pm 1 \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (12)$$

admette, pour Q', R', des valeurs *positives* (*).

11. *Remarque.* Au lieu d'opérer comme il vient d'être dit, on pourrait, dans une des équations

$$QR' \mp 1 = RQ',$$

prendre, arbitrairement, Q, R', puis décomposer le second membre en deux facteurs, *convenablement choisis.*

Soient, par exemple,

$$Q = 37, \quad R' = 17;$$

d'où

$$630 = RQ'.$$

On satisfait, à cette équation, par

$$Q' = 15, \quad R = 42;$$

et ces valeurs sont *convenables* (**).

(*) L'équation

$$37R' - 42Q' = +1$$

n'en admet pas.

(**) Il en résulte, comme ci-dessus,

$$a = 2, 2, 7, 1, 1, 7, 2, 2.$$

III

Série de Lamé.

12. *Un cas particulier.* Supposons que, dans la fraction u, tous les termes soient égaux à 1; et, pour plus de clarté, posons

$$V_2 = 1, 1; \quad V_4 = 1, 1, 1, 1; \quad V_6 = 1, 1, 1, 1, 1, 1; \quad \text{etc.}$$

Nous aurons

$$V_2 = \frac{2}{1}, \quad V_4 = \frac{5}{3}, \quad V_6 = \frac{21}{13}.$$

D'ailleurs, si l'on cherche les réduites successives de V_{2n}, on trouve

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \quad (n > 5).$$

Il est clair (à cause de la loi de formation) que les numérateurs sont les termes de la série de Lamé (*), et qu'il en est de même pour les dénominateurs (abstraction faite du premier).

Si u_n est le $n^{ième}$ terme de la série de Lamé, on a donc

$$V_n = \frac{u_n}{u_{n-1}} \quad \ldots\ldots\ldots\ldots \quad (17)$$

D'ailleurs, la loi de *récurrence* est

$$u_n = u_{n-1} + u_{n-2}, \qquad (n > 2). \quad \ldots\ldots\ldots \quad (18)$$

Avec les notations déjà employées, on a donc :

$$R = u_n, \quad R' = u_{n-1} = Q, \quad R_1 = u_{2n}, \quad R'_1 = u_{2n-1}, \quad Q' = u_{n-2}, \quad Q'_1 = u_{2n-2}; \quad \ldots \quad (19)$$

puis, par les formules (13) :

$$u_{2n} = (u_{n-1})^2 + (u_n)^2, \quad \ldots\ldots\ldots\ldots \quad (20)$$

$$u_{2n-1} = u_{n-1}(u_{n-2} + u_n) \quad \ldots\ldots\ldots\ldots \quad (21)$$

(*) Ou de *Fibonacci*.

Les théorèmes exprimés par ces deux formules nous semblent dignes de remarque. Ils sont dus, en partie, à Édouard Lucas (*).

13. *Remarque.* D'après la formule (21), u_{n-1} divise u_{2n-1}; ou, ce qui revient au même :

Dans la série de Lamé, le terme de rang n *divise le terme de rang* $2n+1$.

14. *Vérifications.* Nous reproduisons ici les quarante-trois premiers termes de la série de Lamé (**).

n	1	2	3	4	5	6	7	8	9	10	11	12	13
u_n	1	2	3	5	8	13	21	34	55	89	144	233	377

n	14	15	16	17	18	19	20
u_n	610	987	1 597	2 584	4 181	6 765	10 946

n	21	22	23	24	25	26
u_n	17 711	28 657	46 368	75 025	121 393	196 418

n	27	28	29	30	31
u_n	317 811	514 229	832 040	1 346 269	2 178 309

n	32	33	34	35
u_n	3 524 578	5 702 887	9 227 465	14 930 352

n	36	37	38	39
u_n	24 157 817	39 088 169	63 245 986	102 334 155

n	40	41	42	43
u_n	165 580 141	267 914 296	433 494 437	701 408 733

(*) *Recherches sur plusieurs ouvrages de Léonard de Pise;* MATHESIS (1887, p. 207), (1889, p. 234). Ce très savant *Arithmologue,* dont la fin prématurée cause tant de regrets, a trouvé bon nombre de théorèmes relatifs à la série de Lamé. Peut-être la modification qu'il a cru devoir faire subir à cette célèbre série l'a-t-elle empêché de les énoncer simplement.

(**) *Notes sur la théorie des fractions continues, etc.*, p. 10. La table publiée dans le beau Mémoire de Lucas, cité ci-dessus, renferme une faute typographique : au lieu de 21 157 817, il faut : 24 157 817.

On doit trouver :

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 34 = 3^2 + 5^2,$$

$$89 = 5^2 + 8^2, \ldots 433\,494\,437 = 10\,946^2 + 17\,711^2 \ (*).$$

De plus :

2 divise 8, 3 divise 21, 5 divise 55, 8 divise 144, ... 17 711 divise 701 408 733 (**).

IV

Généralisation de la série de Lamé (***).

15. ***Préliminaires.*** Soient

$$V_2 = a, a; \qquad V_4 = a, a, a, a; \text{ etc.},$$

a étant un nombre *entier*. En partant de $V_2 = a$, on trouve, comme réduites successives,

$$\frac{a}{1}, \quad \frac{a^2+1}{a}, \quad \frac{a^3+2a}{a^2+1}, \quad \frac{a^4+3a^2+1}{a^3+2a}, \quad \frac{a^5+4a^3+3a}{a^4+3a^2+1}.$$

Ainsi

$$u_n = a u_{n-1} + u_{n-2}, \ldots \ldots \ldots \ldots \quad (22)$$

$$u_1 = a, \qquad u_2 = a^2 + 1, \qquad u_3 = a_3 + 2a, \ldots \ldots \ldots \quad (23)$$

et

$$V_n = \frac{u_n}{u_{n-1}}, \ldots \ldots \ldots \ldots \quad (24)$$

comme ci-dessus (17).

Il est clair que les relations (20), (21) subsistent. On trouve, en effet,

$$a^4 + 3a^2 + 1 = a^2 + (a^2+1)^2,$$

$$a^5 + 4a^3 + 3a = (a^2+1)(a + a^2 + 2a); \text{ etc.}$$

(*) Le premier carré = 119 814 916; le second, 313 679 521, etc.

(**) Le quotient est 39 603 = 10 946 + 28 657. (Voir le tableau ci-contre.)

(***) Les paragraphes III et IV ne font pas double emploi avec ceux qui portent les mêmes titres dans nos *Remarques sur la théorie des fractions continues.*

16. *Limite de* V_n. En la désignant par V, on a, comme on sait,

$$V = a + \frac{1}{V},$$

ou

$$V^2 - aV - 1 = 0;$$

d'où

$$V = \frac{1}{2}(a + \sqrt{a^2 + 4}) \quad \ldots\ldots\ldots\ldots \quad (25)$$

Telle est la limite de la fraction $a, a, a, \ldots$

17. *Remarques.* I. Lorsque a est un nombre entier, cette limite est *incommensurable;* car il n'existe pas de carrés entiers qui diffèrent de 4. Mais, si l'on prend

$$a = \frac{\alpha^2 - \beta^2}{\alpha\beta}, \quad \ldots\ldots\ldots\ldots \quad (26)$$

α et β étant des *nombres entiers,* on aura

$$V = \frac{\alpha}{\beta}.$$

quantité *rationnelle.*

Par exemple, si

$$\alpha = 2, \qquad \beta = 1, \quad \ldots\ldots\ldots\ldots \quad (27)$$

on trouve

$$a = \frac{3}{2}, \quad V = 2.$$

Ainsi, *la fraction continue*

$$\frac{3}{2}, \quad \frac{3}{2}, \quad \frac{3}{2} \ldots$$

a pour limite le nombre 2.

II. a étant une quantité *quelconque,* u_{2n+1} est, *algébriquement,* divisible par u_n; mais, si a est remplacé par une fraction numérique, le terme u_{2n+1} n'est pas, *arithmétiquement,* divisible par u_n (*).

III. a étant un *nombre entier,* les termes de rang *impair,* à partir d'une certaine valeur de n, ne sont pas *premiers.* Par exemple, dans la série de Lamé, *aucun des nombres* 8, 21, 55, ... *n'est premier* (**).

(*) On retrouve ici ce qui est bien connu, relativement à la *divisibilité,* soit *algébrique,* soit *arithmétique.*

(**) Au contraire, dans cette même série, les termes 5, 13, 89, 1 597, ... sont *premiers.*

V

Résidus quadratiques.

18. THÉORÈME. *Le nombre des résidus quadratiques, d'un nombre* p, *premier impair, est* $\frac{p-1}{2}$ (*).

19. COROLLAIRE. Le nombre des non-résidus est, pareillement, $\frac{p-1}{2}$.

20. THÉORÈME. *Tout nombre* p, *premier impair, divise une somme de deux carrés ou de trois carrés, premiers entre eux* (EULER et LAGRANGE).

Soit

$$p = 2k + 1.$$

Nous pouvons former les $\frac{p-1}{2}$ *couples* suivants (**) :

1	2	3	...	$k-1$
$2k-1$	$2k-2$	$2k-3$		$k+1$

1° Si k est résidu, il y a un nombre entier x, inférieur à p, et tel que

$$x^2 = \mathrm{M}(p) + k;$$

ou, en multipliant par 2,

$$2x^2 = \mathrm{M}(p) + p - 1;$$

ou encore

$$x^2 + x^2 + 1 = \mathrm{M}(p) \quad \ldots\ldots\ldots\ldots \quad (28)$$

2° Si $2k = p - 1$ est *résidu,* on a

$$x^2 = \mathrm{M}(p) + p - 1,$$

ou

$$x^2 + 1 = \mathrm{M}(p) \quad \ldots\ldots\ldots\ldots \quad (29)$$

(*) J'omets la démonstration, parce qu'elle est simple et connue. (Voir MATROT, *Journal de Longchamps*, 1892, p. 172.)

(**) Démonstration de M. MATROT, *loc. cit.*

3° Si k et $2k$ sont *non-résidus,* les k résidus se trouvent dans les couples écrits ci-dessus; ce qui exige qu'un de ces couples contienne *deux* résidus. Autrement dit, il existe deux nombres *complémentaires,* α, $2k - \alpha$, et deux carrés, x^2, x'^2, tels que l'on a

$$x^2 = M(p) + \alpha, \qquad x'^2 = M(p) + 2k - \alpha.$$

On conclut, de ces égalités,

$$x^2 + x'^2 = M(p) + 2k = M(p) + p - 1,$$

ou

$$x^2 + x'^2 + 1 = M(p) \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (30)$$

Les égalités (28), (29), (30) prouvent le théorème énoncé.

21. *Remarque. Soient* α, α' *les résidus, par* p, *de deux carrés* x^2, x'^2. *Si* $x^2 + x'^2$ *est divisible par* p, *on a*

$$\alpha + \alpha' = p.$$

En effet,

$$x^2 = M(p) + \alpha, \qquad x'^2 = M(p) + \alpha'.$$

Donc

$$x + x'^2 = M(p) + \alpha + \alpha';$$

ou, à cause de l'hypothèse,

$$\alpha + \alpha' = M(p).$$

Mais, évidemment,

$$\alpha + \alpha' < 2p;$$

ainsi,

$$\alpha + \alpha' = p \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (31)$$

22. *Exemple.* Soient

$$p = 13, \qquad x = 1, \qquad x' = 5, \qquad \alpha = 1, \qquad \alpha' = 12.$$

On a

$$x^2 + x'^2 = 26 = 13 \times 2;$$

et, en conséquence,

$$1 + 12 = 13.$$

23. *Autre remarque. Il peut exister plusieurs couples de résidus, égaux à* p (*).

Ainsi, dans le cas où $p = 13$, les résidus quadratiques sont

$$1, 4, 9, 3, 12, 10, 12, \ldots 1.$$

Or

$$1 + 12 = 3 + 10 = 4 + 9 = 13 \text{ (**)}.$$

VI

Décompositions en carrés.

24. Théorème. *Tout nombre* p, *premier impair, qui divise la somme de deux carrés, premiers entre eux, est la somme de deux carrés* (***).

Supposons que p divise $T^2 + T'^2$, T et T′ étant premiers entre eux. Soit $\frac{S}{S'}$ l'avant-dernière réduite de $\frac{T}{T'}$. Le nombre p divise

$$(T^2 + T'^2)(S^2 + S'^2) = (TS + T'S')^2 + (TS' - ST')^2.$$

Le dernier carré est 1. Donc p divise

$$(TS + T'S' - \alpha p)^2 + 1.$$

(*) J'entends, par là, qu'on peut avoir

$$\alpha + \alpha' = \beta + \beta' = \gamma + \gamma' = \cdots = p.$$

La détermination du nombre de ces couples égaux est, peut-être, un problème difficile à résoudre.

(**) On peut généraliser, en considérant *trois, quatre*... résidus.

A cause de

$$1^2 + 2^2 + 3^2 + \cdots + (p-1)^2 = \frac{(p-1)p(2p-1)}{6},$$

il est presque évident que :

Si p *surpasse* 3, *la somme des* $\frac{p-1}{2}$ *premiers résidus est divisible par* p.

(***) Il est inutile, évidemment, de considérer le nombre $2 = 1^2 + 1^2$.

On peut choisir α de manière que $(ST + S'T' - \alpha p)^2$ soit moindre que p^2. Conséquemment, *il est toujours possible de satisfaire à l'équation*

$$\mu^2 + 1 = pq, \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (32)$$

dans laquelle p est un nombre premier, impair, et μ, un nombre entier, *inférieur à* p (*).

Elle a même forme que

$$Q_1^2 + 1 = R_1 Q_1' \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (15)$$

Donc on y satisfait par

$$\mu = Q_1 = QQ' + RR', \qquad p = R_1 = Q^2 + R^2, \qquad q = Q'^2 + R'^2 \quad . \quad . \quad . \quad (8)$$

25. *Remarque.* Le nombre q est la somme de deux carrés, de même que p. De plus, Q' et R' sont premiers entre eux. Enfin, comme Q et R sont de parités différentes, p a la forme $4k + 1$.

26. COROLLAIRE. *Tout nombre premier, impair, divise un nombre ayant la forme* $\mu^2 + 1$. *En outre,* p — 1 *est résidu quadratique de* p (**).

27. THÉORÈME. *Tout nombre premier* p, *de la forme* $4k + 1$, *est la somme de deux carrés* (FERMAT).

Le théorème précédent (25) peut être considéré comme établissant celui-ci. En voici une autre démonstration, fort ingénieuse, due à M. Hermite (***).

Supposons

$$\mu^2 + 1 = pq \text{ (iv)} \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (32)$$

Réduisons $\frac{p}{\mu}$ en fraction continue. Soient $\frac{M}{M'}$, $\frac{N}{N'}$ deux réduites consécutives, satisfaisant aux conditions

$$M < \sqrt{p}, \qquad N > \sqrt{p}.$$

(*) S'il en est ainsi, $p - 1$ est résidu quadratique de p.

(**) La première partie a été démontrée ci-dessus [20].

(***) *Journal de Liouville,* 1848. Nous essayons de la réduire un peu, et de la compléter.

(iv) L'illustre Géomètre, qui était bien jeune en 1848, aurait dû, peut-être, *prouver* ou *rappeler* la possibilité de cette équation (32). Aujourd'hui, il serait moins laconique.

Les réduites correspondantes de $\frac{\mu}{p}$ seraient $\frac{M'}{M}$, $\frac{N'}{N}$. Donc, suivant le cas,

$$\frac{\mu}{p} - \frac{M'}{M} < \frac{1}{MN}, \quad \frac{M'}{M} - \frac{\mu}{p} < \frac{1}{MN}.$$

Ces deux formules sont comprises dans celle-ci :

$$\left(\frac{\mu}{p} - \frac{M'}{M}\right)^2 < \frac{1}{M^2N^2},$$

ou

$$(M\mu - M'p)^2 < \frac{p^2}{N^2} \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (18)$$

Mais N^2 surpasse p. Donc, à plus forte raison,

$$(M\mu - M'p)^2 < p ;$$

puis, à cause de $M^2 < p$:

$$(M\mu - M'p)^2 + M^2 < 2p.$$

D'après l'égalité (32), le premier membre est un multiple de p. Et puisqu'il est inférieur à $2p$, il ne peut différer de p. Autrement dit :

$$p = (M\mu - M'p)^2 + M^2 \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (33)$$

C. Q. F. D.

28. *Remarque.* L'équation (33), développée, est, si l'on tient compte de la condition (32),

$$M'^2p^2 - 2MM'\mu p + M^2qq = p,$$

ou

$$M'^2p - 2MM'\mu + M^2q = 1. \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (34)$$

On tire, de celle-ci :

$$M'^2p = 1 + 2MM'\mu - M^2q \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (35)$$

29. *Vérification.* Nous avons trouvé

$$p = Q^2 + R^2, \qquad \mu = QQ' + RR', \qquad q = Q'^2 + R'^2.$$

Donc l'équation (35) est la même chose que

$$M'^2(Q^2 + R^2) - 2MM'(QQ' + RR') + M^2(Q'^2 + R'^2) = 1,$$

ou

$$(M'Q - MQ')^2 + (M'R - MR')^2 = 1 \quad \ldots\ldots\ldots \quad (36)$$

Celle-ci est réductible aux deux systèmes suivants :

$$(M'Q - MQ')^2 = 1, \qquad M'R - MR' = 0;$$

$$M'Q - MQ' = 0, \qquad (M'R - MR')^2 = 1.$$

Le premier donne

$$\frac{M}{M'} = \frac{R}{R'};$$

ce qui est inadmissible; car la réduite $\frac{N}{N'}$ n'*existerait pas*. Le second système conduit à

$$\frac{M}{M'} = \frac{Q}{Q'}, \quad \frac{N}{N'} = \frac{R}{R'}. \quad \ldots\ldots\ldots\ldots \quad (37)$$

Ainsi, dans la démonstration donnée précédemment (*), on doit avoir

$$M = Q < \sqrt{p}, \qquad N = R > \sqrt{p} \quad \ldots\ldots\ldots \quad (38)$$

30. *Application.* Soit $\frac{p}{\mu} =$

$$3,\quad 2,\quad 5,\quad 4,\quad 2,\quad 2,\quad 4,\quad 5,\quad 2,\quad 3.$$

Les réduites sont

$$\frac{3}{1},\ \frac{7}{2},\ \frac{58}{11},\ \frac{159}{46},\ \frac{356}{103},\ \frac{871}{252},\ \frac{5\,840}{1\,111},\ \frac{20\,071}{58\,071},\ \frac{48\,982}{12\,725},\ \frac{152\,017}{43\,982},$$

Donc

$$q = 4, \qquad r = 2, \qquad Q = 159, \qquad Q' = 46, \qquad R = 356, \qquad R' = 103,$$

$$p = 152\,017\ (**), \qquad \mu = 43\,982, \qquad q = 12\,725.$$

(*) Celle de M. Hermite.

(**) Le nombre 152 017 est *premier*. (*Table de Burckhard*, p. 17.)

31. THÉORÈME. *Si un nombre premier,* p, *n'est pas la somme de deux carrés,* p^2 *est la somme de trois carrés* (*).

1° Supposons

$$p = a^2 + b^2 + c^2.$$

On a, identiquement,

$$p^2 = (a^2 + b^2 + c^2)^2 = (a^2 + b^2 - c^2)^2 + (2ac)^2 + (2bc)^2. \quad . \quad . \quad . \quad . \quad (39)$$

On ne peut avoir, ni $c = 0$, ni $c^2 = a^2 + b^2$; car, dans le premier cas, p serait la *somme de deux carrés;* et, dans le second, ce nombre *impair* serait égal à $2(a^2 + b^2)$.

2° Soit, maintenant,

$$p = a^2 + b^2 + c^2 + d^2;$$

puis

$$p^2 = (a^2 + b^2 - c^2 - d^2)^2 + 4(a^2 + b^2)(c^2 + d^2).$$

Le dernier terme est réductible à $(2f)^2 + (2g)^2$, en faisant

$$f = ac \pm bd, \qquad g = ad \mp bc \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (40)$$

Ainsi

$$p^2 = (a^2 + b^2 - c^2 - d^2)^2 + [2(ac \pm bd)]^2 + [2(ad \mp bc)]^2 \quad . \quad . \quad . \quad . \quad (41)$$

On ne peut supposer

$$c^2 + d^2 = a^2 + b^2;$$

car p serait *pair*.

Si $ac = bd$, on a

$$p = a^2 + b^2 + c^2 + d^2 \pm 2ac \mp 2bd,$$

ou

$$p = (a \pm c)^2 + (b \mp d)^2,$$

contre l'hypothèse. Même conclusion si $ad = bc$ (**).

(*) Dans les *Recherches sur quelques produits indéfinis* (1873), j'ai conclu ce théorème, de la considération des *séries elliptiques*. Il restait à le démontrer d'une manière élémentaire.

(**) D'après le théorème de Bachet (voir plus loin), il est inutile de supposer p égal à la somme de *cinq* carrés, de *six* carrés, etc.

32. *Remarque.* Un nombre premier, de la forme $4k - 1$, peut être, à la fois, la somme de *trois* carrés et la somme de *quatre* carrés.

Exemple :

$$19 = 9 + 9 + 1 = 16 + 1 + 1 + 1.$$

33. *Suite.* Dans ce même cas, p^2, somme de trois carrés, peut être la somme de *quatre* carrés.

Exemple. Soit

$$p = 19.$$

On a

$$p^2 = 361 = 17^2 + 6^2 + 6^2 = 16^2 + 10^2 + 2^2 + 1^2.$$

34. THÉORÈME. *Tout nombre premier,* p, *divise une somme de deux, trois ou quatre carrés, premiers entre eux* (*).

Considérons, seulement, les deux derniers cas.

On peut toujours, le nombre p étant donné, satisfaire à l'équation

$$x^2 + x'^2 + 1 = \mathrm{M}(p), \quad \ldots\ldots\ldots\ldots \quad (30)$$

dans laquelle x et x' sont inférieurs à p.

Si l'on ajoute p^2 aux deux membres, on a

$$x^2 + x'^2 + 1 + p^2 = \mathrm{M}(p).$$

La première équation a la forme

$$\mathrm{A}^2 + \mathrm{B}^2 + \mathrm{C}^2 = \mathrm{M}(p); \quad \ldots\ldots\ldots\ldots \quad (42)$$

et la seconde, celle-ci :

$$\mathrm{A}^2 + \mathrm{B}^2 + \mathrm{C}^2 + \mathrm{D}^2 = \mathrm{M}(p) \quad \ldots\ldots\ldots\ldots \quad (43)$$

C. Q. F. D.

35. *Remarque.* L'équation (43) est, comme on l'a vu, réductible à

$$a^2 + b^2 + c^2 + d^2 = \mathrm{M}(p); \quad \ldots\ldots\ldots\ldots \quad (44)$$

a, b, c, d étant des *résidus quadratiques,* moindres, en valeurs absolues, que $\frac{p}{2}$.

(*) Cette proposition, *essentielle,* a été omise par Legendre. On la trouve dans l'*Algèbre supérieure,* de Serret (t. II, p. 98).

36. Lemme. $a, b, c, d, a', b', c', d'$ étant des nombres quelconques, on a, identiquement,

$$\left.\begin{aligned}&(a^2+b^2+c^2+d^2)(a'^2+b'^2+c'^2+d'^2)=\\&(aa'+bb'+cc'+dd')^2+(ab'-ba'+cd'-dc')^2\\&+(ac'-ca'+db'-bd')^2+(ab'-ba'+bc'-cb')^2\end{aligned}\right\}\ (*).\quad\ldots\quad(45)$$

37. *Remarque. Si l'on suppose*

$$a^2+b^2+c^2+d^2=nq,$$

$$a'=a-n\alpha,\qquad b'=b-n\beta,\qquad c'=c-n\gamma,\qquad d'=d-n\delta,$$

n, q, α, β, γ, δ *étant des nombres entiers, on a*

$$aa'+bb'+cc'+dd'=nq-n(a\alpha+b\beta+c\gamma+d\delta),$$

$$ab'-ba'=n(b\alpha-\alpha\beta);\ \text{etc.}$$

En conséquence

$$(a^2+b^2+c^2+d^2)(a'^2+b'^2+c'^2+d'^2)=\left[\mathrm{M}(n)\right]^2,$$

ou

$$q(a'^2+b'^2+c'^2+d'^2)=\mathrm{M}(n)\quad\ldots\quad(46)$$

38. Théorème. *Tout nombre premier impair, qui divise une somme de quatre carrés, premiers entre eux, non réductible* (**), *est la somme de trois ou de quatre carrés.*

Soit

$$\mathrm{N}=\mathrm{A}^2+\mathrm{B}^2+\mathrm{C}^2+\mathrm{D}^2=\mathrm{M}(p).\quad\ldots\quad(47)$$

Divisons, par p, les nombres entiers A, B, C, D, en prenant chacun des quotients par défaut ou par excès, de manière que le reste correspondant soit, en valeur absolue, inférieur à $\frac{1}{2}p$.

Nous pouvons écrire, au lieu de cette égalité,

$$a^2+b^2+c^2+d^2=pq,\quad\ldots\quad(48)$$

(*) Identité d'Euler.

(**) Cela signifie que le dividende, s'il est la somme de *quatre* carrés, n'est pas la somme de *trois* carrés ou de *deux* carrés; etc.

q étant un nombre entier, et les carrés a^2, b^2, c^2, d^2 satisfaisant aux conditions

$$a^2 < \frac{1}{4}p^2, \quad b^2 < \frac{1}{4}p^2, \ \ldots$$

Si

$$q = 1,$$

l'équation se réduit à

$$p = a^2 + b^2 + c^2 + d^2.$$

Ainsi, le nombre p serait la somme de *quatre* carrés, au plus; et le théorème serait démontré. Supposons donc $q > 1$.

Nous avons

$$pq < 4\left(\frac{p}{2}\right)^2,$$

ou

$$q < p. \quad \ldots\ldots\ldots\ldots\ldots \quad (49)$$

Le quotient q divise

$$a^2 + b^2 + c^2 + d^2;$$

donc il divise

$$(a - \alpha q)^2 + (b - \beta q)^2 + (c - \gamma q)^2 + (d - \delta q)^2.$$

On peut choisir les entiers α, β, γ, δ, de manière que chaque carré soit inférieur à $\frac{1}{4}q^2$. Ainsi, sous forme abrégée,

$$a'^2 + b'^2 + c'^2 + d'^2 = qq', \quad \ldots\ldots\ldots \quad (50)$$

avec la condition

$$q' < q; \quad \ldots\ldots\ldots\ldots\ldots \quad (51)$$

puis, à cause de l'égalité (48),

$$(a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2) = pq^2p' \quad \ldots\ldots \quad (52)$$

On a vu, précédemment [37], que le premier membre est divisible par q^2. La suppression de ce facteur donne une nouvelle équation :

$$a''^2 + b''^2 + c''^2 + d''^2 = pq' \quad \ldots\ldots\ldots \quad (53)$$

Si $q' = 1$, on a

$$p = a''^2 + b''^2 + c''^2 + d''^2;$$

le théorème est démontré.

Mais l'équation (53) a même forme que l'équation (50). Donc, l'application du procédé employé donnera une équation

$$a'''^2 + b'''^2 + c'''^2 + d'''^2 = pq'', \quad \ldots\ldots\ldots \quad (54)$$

avec la condition

$$q'' < q'.$$

Les nombres *entiers* q, q', q'', ... allant en diminuant, le dernier d'entre eux sera 1. C. Q. F. D. (*).

39. *Application numérique.* Soient

$$A = 48, \quad B = 59, \quad C = 62, \quad D = 83;$$

de sorte que

$$N = 2\,304 + 3\,481 + 3\,844 + 6\,889 = 16\,518.$$

N est divisible par le nombre premier 2 753. Ainsi, il faut décomposer 2 753 en trois ou quatre carrés.

Évidemment,

$$a = A, \quad b = B, \quad c = C, \quad d = D;$$

puis

$$q = 6.$$

Ensuite,

$$a' = \pm(48 - 6\alpha), \quad b' = \pm(59 - 6\beta), \quad c' = \pm(62 - 6\gamma), \quad d' = \pm(83 - 6\delta);$$

puis

$$a' = 0, \quad b' = -1, \quad c' = 2, \quad d' = -1.$$

(*) Cette démonstration est due, je crois, à Legendre. Mais, dans la *Théorie des Nombres*, elle est un peu difficile à suivre. De plus, l'illustre Géomètre suppose que tout nombre entier N, admet un diviseur premier, supérieur à $\sqrt{N}$; ce qui n'est pas. Voir, sur ce point, les *Mélanges mathématiques*, t. III, p. 160.

L'équation (50) est

$$1 + 4 + 1 = 6q',$$

ou

$$q' = 1.$$

On trouve ensuite, par les formules du n° 37,

$$a'' = -18, \qquad b'' = -276, \qquad c'' = 72, \qquad d'' = 132.$$

Par conséquent,

$$18^2 + 276^2 + 72^2 + 132^2 = 6^2 p,$$

ou

$$p = 3^2 + 46^2 + 12^2 + 22^2 = 9 + 2116 + 144 + 184 = 2753;$$

ce qui est exact.

40. Théorème de Bachet. *Tout nombre entier est carré ou est la somme de deux, trois ou quatre carrés.*

1° Soit

$$N = p^\beta q^\gamma r^\delta \dots,$$

p, q, r étant premiers, *impairs*.

On vient de voir que chacun de ces facteurs, p, par exemple, est la somme de *quatre* carrés, au plus. Donc, par l'identité d'Euler (36), si N n'est pas carré, ce nombre est la somme de *deux*, *trois* ou *quatre* carrés.

2° Si

$$N = 2^\alpha p^\beta q^\gamma r^\delta + \dots,$$

comme

$$2 = 1^2 + 1^2,$$

est la somme de *deux* carrés : la conclusion subsiste.

VII

Sur une Note de M. Matrot.

41. I. Au *Congrès de Marseille* (1891), M. Matrot a communiqué une démonstration, fort remarquée, du théorème de Bachet. Je ne la crois pas à l'abri de toute critique. De plus, la Note du savant Ingénieur, publiée dans le *Journal de Longchamps* (1891, p. 169), contient bon nombre de fautes typographiques (*).

II. Dans son *Aperçu historique sur le théorème de Bachet*, M. Matrot énonce ce théorème *empirique* d'Euler (**) :

Un entier ne peut se décomposer en quatre carrés fractionnaires, que s'il est décomposable en quatre carrés entiers.

Ce théorème me paraît *faux*. Je crois, en effet, avoir démontré celui-ci :

Tout nombre entier est, d'une infinité de manières, décomposable en quatre carrés fractionnaires (***).

Par exemple,

$$5 = \left(\frac{5}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2$$

$$= \left(\frac{8}{5}\right)^2 + \left(\frac{5}{5}\right)^2 + \left(\frac{1}{5}\right)^2 + \left(\frac{1}{5}\right)^2$$

$$= \left(\frac{12}{7}\right)^2 + \left(\frac{1}{7}\right)^2 + \left(\frac{1}{7}\right)^2 + \left(\frac{1}{7}\right)^2,$$

etc.

III. La démonstration donnée par M. Matrot a été l'occasion du présent travail.

(*) Voir, par exemple, les deux premières lignes de la page 170.
(**) Congrès de Marseille, p. 289.
(***) *Mélanges mathématiques*, t. III, p. 165.

Liége, août-octobre 1893.

P. S.

Dans la démonstration donnée page 21, rien n'exprime que p est un nombre *premier*. Donc :

1° *Si un nombre impair,* N, *non carré, n'est pas la somme de deux carrés,* N^2 *est la somme de trois carrés;* ou, par le théorème de Bachet :

Si un nombre impair, N, *est la somme de trois carrés ou de quatre carrés,* N^2 *est la somme de trois carrés;* puis, évidemment : *chacun des nombres* N^4, N^8, N^{16}, ... *est la somme de trois carrés;*

2° Pour passer au cas où N est *pair,* il suffit de multiplier, par 4, 16, 64, . . les deux membres des égalités (39), (41).

Le théorème peut donc être ainsi énoncé :

Si un nombre N *est la somme de trois carrés ou de quatre carrés,* N^2 *est la somme de trois carrés.*

9 novembre 1893.