JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

V.-A. LEBESGUE

Démonstration de quelques formules d'un mémoire de M. Jacobi

Journal de mathématiques pures et appliquées 1re série, tome 19 (1854), p. 289-300.
<http://www.numdam.org/item?id=JMPA_1854_1_19__289_0>

DÉMONSTRATION

DE

QUELQUES FORMULES D'UN MÉMOIRE DE M. JACOBI[*];

PAR M. V.-A. LEBESGUE.

Le Mémoire de Jacobi est extrait d'une Lettre adressée à l'Académie des Sciences de Berlin en 1837. Voici les premières lignes :

« Soit x une racine de l'équation $\frac{x^p-1}{x-1}=0$, où p est un nombre » premier. Le nombre g étant une racine primitive de p, si l'on pose

$$F(\alpha)=x+\alpha x^g+\alpha^2 x^{g^2}\ldots+\alpha^{p-2}x^{g^{p-2}},$$

» où α est une racine quelconque de l'équation $\frac{\alpha^{p-1}-1}{\alpha-1}=0$, on aura

$$F(\alpha).F(\alpha^{-1})=\alpha^{\frac{p-1}{2}}.p,$$

$$F(\alpha^m).F(\alpha^n)=\psi(\alpha).F(\alpha^{m+n});$$

» $\psi(\alpha)$ sera une fonction entière à coefficients entiers de α. On a, de » plus,

$$\psi(\alpha).\psi(\alpha^{-1})=p.$$

» Si r représente une racine primitive de la congruence $r^{p-1}\equiv 1 \pmod p$, » et que l'on mette dans la fonction

$$\psi(r)=\frac{F(r^{-m}).F(r^{-n})}{F(r^{-m-n})}$$

» pour r le nombre g, on aura, m et n étant positifs et plus petits

[*] *Journal de Mathématiques* de M. Crelle, tome XXX, page 166.

que $p-1$,

$$\psi(g) \equiv -\frac{\Pi(m+n)}{\Pi m\ \Pi n} \pmod{p},$$

» où $\Pi m = 1.2.3\ldots m$. Quand on a $m+n > p-1$, $\psi(g)$ est » $\equiv 0 \pmod{p}$. Ce théorème doit être regardé comme un des plus » importants pour les applications. J'ai communiqué ces théorèmes à » M. Gauss depuis plus de dix ans. »

Voici les démonstrations de ces beaux théorèmes, M. Cauchy les a données dans les Notes première et cinquième de son Mémoire sur la Théorie des Nombres. (Ce Mémoire, qui est de 1830, a paru avec des Notes fort étendues dans le tome XVII des *Mémoires de l'Académie des Sciences*, 1840.) Les démonstrations sont ici réduites à peu de pages, et avec quelques modifications de nature à les simplifier; elles conviendront à un plus grand nombre de lecteurs.

PROPOSITION I. *Le produit* $F(\alpha).F(\alpha^{-1})$ *est toujours égal à* $\alpha^{\frac{p-1}{2}}.p$, α *étant autre que l'unité.*

Démonstration. Ordonnons le produit suivant les puissances de α; d'abord le terme en α^0 sera

$$x^2 + x^{2g} + x^{2g^2} + \ldots + x^{2g^{p-2}}.$$

Or $2, 2g, \ldots, 2g^{p-2}$, en ôtant les multiples de p, se réduisent, à l'ordre près, à

$$2,\ 4,\ 6,\ldots,\ 2(p-1), \quad \text{ou} \quad 1,\ 2,\ldots,\ p-1;$$

mais

$$1 + x + x^2 \ldots + x^{p-1} = 0;$$

le coefficient est donc -1. Le terme en α est

$$\left(x^{g^0+g^1} + x^{g^1+g^2} + x^{g^2+g^3} \ldots + x^{g^{p-2}+g^0}\right)\alpha;$$

si l'on pose

$$g^0 + g^1 = 1 + g = n,$$

il deviendra

$$\left(x^n + x^{ng} + \ldots + x^{ng^{p-2}}\right)\alpha, \quad \text{ou} \quad -\alpha.$$

On en dira autant des autres termes; seulement, dans le multiplicateur

de $\alpha^{\frac{p-1}{2}}$, les exposants $1+g^{\frac{p-1}{2}}$, $g\left(1+g^{\frac{p-1}{2}}\right)$, etc., étant multiples de p, ce multiplicateur deviendra $p-1$, et comme

$$1+\alpha+\ldots+\alpha^{p-2}=\frac{\alpha^{p-1}-1}{\alpha-1}=0,$$

on aura finalement

$$F(\alpha).F(\alpha^{-1})=p\alpha^{\frac{p-1}{2}}.$$

PROPOSITION II. *Soient α, β deux racines de $\frac{\alpha^{p-1}-1}{\alpha-1}=0$, et telles qu'on n'ait pas $\alpha\beta=1$, on aura toujours*

$$F(\alpha)F(\beta)=F(\alpha\beta).\sum_{s=1}^{s=p-2}\alpha^{\operatorname{ind} s}(\alpha\beta)^{-\operatorname{ind}(s+1)}.$$

J'ai modifié l'énoncé; celui qui précède montre la formation du facteur $\psi(\alpha)$. On sait que $\operatorname{ind} s$ (indice de s) est un entier, tel qu'on a

$$g^{\operatorname{ind} s}\equiv s\pmod p.$$

L'entier s sera supposé positif $<p$, et autre que zéro. Le *Canon arithmeticus* de Jacobi donne ces indices pour tous les modules premiers inférieurs à 1000.

Démonstration. Le terme général du produit est

$$\alpha^i\beta^k x^{g^i+g^k}.$$

Soit d'abord

$$x^{g^i+g^k}=1,$$

il faudra avoir

$$g^i+g^k\equiv 0\pmod p \quad \text{ou} \quad 1+g^{i-k}\equiv 0;$$

mais

$$1+g^{\frac{p-1}{2}}\equiv 0, \quad \text{ainsi} \quad k=i\pm\frac{p-1}{2};$$

de sorte que

$$\alpha^i\beta^k=(\alpha\beta)^i\alpha^{\pm\frac{p-1}{2}}.$$

D'abord $\alpha^{p-1}=1$ donne

$$\alpha^{\frac{p-1}{2}}=\alpha^{-\frac{p-1}{2}},$$

ainsi l'on a toujours

$$\alpha^i\beta^k = (\alpha\beta)^i\alpha^{\frac{p-1}{2}},$$

et, comme on doit faire

$$i = 0,\ 1,\ 2,\ldots,\ p-2,$$

la somme

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

sera nulle.

Soit ensuite

$$g^i + g^k \equiv g^m \quad \text{ou bien} \quad 1 + g^{i-k} \equiv g^{m-k} \pmod{p};$$

en posant

$$g^{i-k} \equiv s, \quad \text{d'où} \quad g^{m-k} \equiv s+1,$$

il viendra

$$i - k \equiv \operatorname{ind} s, \quad m - k \equiv \operatorname{ind}(s+1), \quad \pmod{p-1};$$

de sorte que le coefficient $\alpha^i\beta^k$ devient, à cause de $k \equiv m - \operatorname{ind}(s+1)$, $i \equiv k + \operatorname{ind} s \equiv m + \operatorname{ind} s - \operatorname{ind}(s+1)$,

$$(\alpha\beta)^{m-\operatorname{ind} s\,(s+1)}\,.\,\alpha^{\operatorname{ind} s},$$

et le terme complet sera

$$(\alpha\beta)^m\,.\,x^{g^m}\sum_{s=1}^{s=p-2}\alpha^{\operatorname{ind} s}\,.\,(\alpha\beta)^{-\operatorname{ind} s\,(s+1)}.$$

La somme S ne varie pas, quel que soit m; elle doit être prise pour

$$s = 1,\ 2,\ldots,\ p-2;$$

de sorte que l'on a la formule de l'énoncé en donnant à m les valeurs $0,\ 1,\ 2,\ldots,\ p-2$, et faisant la somme des résultats.

Si l'on avait posé

$$1 + g^{k-i} = g^{m-i},$$

puis

$$g^{k-i} = s' \quad [\text{de là} \quad ss' \equiv 1 \pmod{p}],$$

on aurait trouvé

$$\mathrm{F}(\alpha\beta)\sum_{s'=1}^{s'=p-2}\beta^{\operatorname{ind} s'}\,.\,(\alpha\beta)^{-\operatorname{ind}(s'+1)},$$

En effet, comme $ss' \equiv 1$ donne $s(s'+1) \equiv 1+s$, on a à la fois

$$\operatorname{ind} s + \operatorname{ind} s' \equiv 0 \quad \text{et} \quad \operatorname{ind} s + \operatorname{ind}(s'+1) \equiv \operatorname{ind}(s+1) \pmod{p-1},$$

d'où résulte

$$S\alpha^{\operatorname{ind} s}(\alpha\beta)^{-\operatorname{ind}(s+1)} = S\beta^{\operatorname{ind} s'}.(\alpha\beta)^{-\operatorname{ind}(s'+1)}.$$

Corollaire. Si l'on fait

$$\alpha = \gamma^m, \qquad \beta = \gamma^n,$$

on aura

$$\psi(\gamma) = S.\gamma^{m\operatorname{ind} s - (m+n)\operatorname{ind}(s+1)},$$

et l'équation

$$F(\gamma^m).F(\gamma^n) = \psi(\gamma).F(\gamma^{m+n}),$$

qui est celle de Jacobi.

Cette démonstration est prise en partie à M. Cauchy. La notation se rapproche de celle d'Eisenstein. M. Kummer a donné encore d'autres formes au nombre complexe $\psi(\gamma)$.

La proposition II suppose donc qu'on n'a pas

$$\gamma^m = 1, \gamma^n = 1, \ \gamma^{m+n} = 1 \qquad (\alpha = 1, \ \beta = 1, \ \alpha\beta = 1).$$

Proposition III. *On a toujours l'équation*

$$p = S\alpha^{\operatorname{ind} s}(\alpha\beta)^{-\operatorname{ind}(s+1)}.S\alpha^{-\operatorname{ind} s}(\alpha\beta)^{\operatorname{ind}(s+1)},$$

les sommes étant prises pour $s = 1, 2, \ldots, p-2$.

Démonstration. Changez, dans la proposition II, α, β en α^{-1}, β^{-1}; multipliez membre à membre les équations ainsi obtenues, et simplifiez, par le moyen de la proposition I, et vous aurez l'équation de la proposition III.

Corollaire I. Si les racines α, β étaient changées en α^m, α^n, on aurait

$$p = S\alpha^{m\operatorname{ind} s - (m+n)\operatorname{ind}(s+1)}.S\alpha^{-m\operatorname{ind} s + (m+n)\operatorname{ind}(s+1)}.$$

Corollaire II. Soit

$$p = \mu\varpi + 1, \qquad \alpha^\mu = 1,$$

et, de plus,

$$m = 1, \quad m + n = \mu - 1, \quad \text{ou} \quad n = \mu - 2,$$

on trouvera

$$p = S\alpha^{\text{ind } s\,(s+1)} . S\alpha^{-\text{ind } s\,(s+1)} = p_1 p_2;$$

on a donc

$$p_1 = S\alpha^{\text{ind } s\,(s+1)} = a_0 + a_1\alpha + a_2\alpha^2 + \dots a_{\mu-1}\alpha^{\mu-1}.$$

D'où cette règle : Prenez, dans le *Canon arithmeticus* de Jacobi, les indices des nombres 2, 6, 12,..., $(p-2)$, $(p-1)$ (doubles des nombres triangulaires), le coefficient a_i représentera le nombre des indices de forme $k\mu + i$. Cette règle est d'Eisenstein.

PROPOSITION IV. *Si dans*

$$\frac{F(r^{-m}).F(r^{-n})}{F(r^{-m-n})} = \psi(r)$$

le nombre r racine primitive de $r^{p-1} \equiv 1 \pmod p$ *est remplacé par le nombre g, on aura, m et n étant positifs inférieurs à* $p-1$ *et* $m+n$ *non divisible par* $p-1$,

$$\psi(g) \equiv -\frac{\Pi(m+n)}{\Pi m.\Pi n} \pmod p.$$

Démonstration. Si dans les propositions I et II on remplace α, β par les entiers g^{-m}, g^{-n}, les démonstrations subsistent, seulement les équations se changent en congruences pour le module p.

Le nombre qui multiplie $F(g^{-m-n})$ n'est autre que le coefficient de x^1, c'est-à-dire $Sg^{-mi}.g^{-nk}$ sous l'hypothèse $g^i + g^k \equiv 1$, ou encore $S.g^{-mi}(1-g^i)^{-n}$ qui revient à

$$Sg^{(p-1-m)i}(1-g^i)^{p-1-n}.$$

Posons

$$p-1-m = m_1, \quad p-1-n = n_1;$$

comme le terme général de S est

$$(-1)^h \frac{n_1(n_1-1)\dots(n_1-h+1)}{1.2\dots h} g^{i(m_1+h)},$$

et que, pour avoir le reste de S divisé par p, on doit remplacer

$1 + g^k + g^{2k} \ldots + g^{(p-2)k} = \frac{g^{(p-1)k} - 1}{g^k - 1}$ par 0 ou $p - 1$, selon que k est ou non multiple de $p - 1$, il faudra poser

$$m_1 + h = p - 1 \quad \text{ou bien} \quad h = p - 1 - m_1 = m :$$

on aura ainsi

$$(-1)^m (p-1) \frac{[p-(n+1)].[p-(n+2)]\ldots[p-(n+m)]}{1.2\ldots m}$$

$$\equiv -(-1)^m \frac{pQ + (-1)^m (n+1)(n+2)\ldots(n+m)}{1.2\ldots m}$$

$$\equiv -\frac{(n+1)(n+2)\ldots(n+m)}{1.2\ldots m} \equiv -\frac{\Pi(m+n)}{\Pi m . \Pi n} \pmod{p}.$$

N. B. Q est un entier que l'on peut négliger, parce que $\frac{(n+1)(n+2)\ldots(n+m)}{1.2\ldots m}$ est entier. Comme $i = 0$ donne $1 - g^i = 0$, il a été permis de faire $i = 0$. Sans cela, la chose n'aurait pas été permise.

On pourrait tirer de là les formules de M. Cauchy pour les coefficients du nombre $\psi(\alpha)$ qui sont précisément les mêmes que ceux de $\psi(g)$.

Dans le nombre

$$a_0 + a_1 \alpha + a_2 \alpha^2 + \ldots a_{\mu-1} \alpha^{\mu-1} \quad \text{où} \quad \mu = \frac{p-1}{\varpi},$$

si nous faisons $\alpha = \rho^\varpi$, ρ étant une racine primitive, nous aurons, par le théorème précédent, la valeur de

$$a_0 + a_1 g^\varpi + a_2 g^{2\varpi} + \ldots a_{\mu-1} g^{(\mu-1)\varpi};$$

mais le changement de α, β en g^{-m}, g^{-n} pouvant être remplacé par celui de α, β en g^{-mi}, g^{-ni}, on obtiendrait assez de congruences pour déterminer $a_0, a_1, \ldots, a_{\mu-1}$. Il serait inutile de les mettre ici et de faire quelques remarques relatives aux cas pour lesquels la proposition II est en défaut. Tout ce qu'il importe de remarquer, c'est que a_0, a_1, etc., dépendent de congruences du premier degré, renfermant des coefficients binomiaux. De là résulte ce beau théorème :

Toutes les équations indéterminées auxquelles on est conduit par

la formule

$$p = \psi(\alpha).\psi(\alpha^{-1})$$

sont résolubles algébriquement au moyen des restes de certains coefficients binomiaux.

Le premier exemple est dû à M. Gauss, qui a montré que l'équation

$$x^2 + y^2 = p = 4\varpi + 1$$

est résolue en prenant

$$x \equiv \frac{1}{2}\frac{\Pi\ 2\varpi}{\Pi\varpi.\Pi\varpi} \pmod{p}.$$

M. Jacobi et surtout M. Cauchy en ont donné d'autres.

On voit en quoi consiste l'importance que M. Jacobi donne à la proposition IV.

Application de la proposition III, objet principal de cette Note.

On a

$$p = S\alpha^{m \operatorname{ind} s - (m+n) \operatorname{ind}(s+1)}.\ S\alpha^{-m \operatorname{ind} s + (m+n) \operatorname{ind}(s+1)}.$$

Si l'on suppose

$$p = \mu\varpi + 1 \quad \text{et} \quad \alpha^{\mu} = 1,$$

au moyen du *Canon arithmeticus*, on formera facilement l'équation

$$p = f(\alpha).f(\alpha^{-1})$$

$$= (a_0 + a_1\alpha + \ldots + a_{\mu-1}\alpha^{\mu-1})(a_0 + a_1\alpha^{-1} + a_2\alpha^{-2} \ldots + a_{\mu-1}\alpha^{-(\mu-1)}),$$

ou bien encore

$$p = A_0 + A_1\alpha + A_2\alpha^2 \ldots + A_{\mu-1}\alpha^{(\mu-1)},$$

en posant

$$A_0 = \Sigma a_i^2, \quad A_1 = \Sigma a_i a_{i+1}, \ldots, \quad A_k = \Sigma a_i a_{i+k}, \ldots,$$

les sommes étant prises en faisant $i = 0, 1, 2, \ldots, \mu - 1$ et diminuant, quand cela est possible, les indices de μ.

Ainsi l'on a l'équation

$$P = A_0 - p + A_1 \alpha + A_2 \alpha^2 + \ldots + A_{\mu-1} \alpha^{(\mu-1)} = 0.$$

Remarque. En partant de l'équation

$$p = S\alpha^{\text{ind } s\,(s+1)} \cdot S\alpha^{-\text{ind } s\,(s+1)},$$

le calcul des a_0, a_1, etc., et, par suite, des A_0, A_1, etc., devient très-facile au moyen de la règle de M. Eisenstein, donnée plus haut.

Ceci posé, comme l'équation $P = 0$ est satisfaite par toutes les valeurs de α autres que celles qui satisfont à

$$\alpha^m = 1, \quad \alpha^n = 1, \quad \alpha^{m+n} = 1,$$

on saura trouver une fonction entière de α, savoir

$$Q = B_0 + B_1 \alpha + B_2 \alpha_2 + \ldots + B_\nu \alpha^\nu,$$

qui divisera P; de là des équations de condition entre les coefficients de l'équation $P = 0$. Comme $Q = 0$ n'a pas de racines égales, si le reste de la division de P par Q est

$$C_0 + C_1 \alpha + \ldots + C_{\nu-1} \alpha^{\nu-1},$$

il faudra poser

$$C_0 = 0, \quad C_1 = 0, \ldots, \quad C_{\nu-1} = 0.$$

On peut évidemment, pour simplifier, remplacer Q par un de ses diviseurs, on obtient ainsi des équations de condition plus simples et qui résultent des conditions générales.

Dans le cas présent, si ω_1, ω_2, ω_3 sont les plus grands communs diviseurs de μ et m, μ et n, μ et $m + n$, et que ω soit le plus petit multiple de ω_1, ω_2, ω_3 (supposé autre que μ), on pourra prendre pour Q le quotient

$$\frac{\alpha^\mu - 1}{\alpha^\omega - 1} \quad \text{ou} \quad \alpha^{\mu-\omega} + \alpha^{\mu-2\omega} + \ldots + \alpha^\omega + 1 = 0.$$

Les équations de condition deviennent

$$A_0 - p = A_\omega = A_{2\omega} \ldots = A_{\mu-\omega},$$
$$A_1 = A_{\omega+1} = A_{2\omega+1} \ldots = A_{\mu-\omega+1},$$
$$A_2 = A_{\omega+2} = A_{2\omega+2} \ldots = A_{\mu-\omega+2},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

En doublant les équations de la première ligne, il vient

$$2p = 2A_0 - 2A_{f\omega},$$

où f peut être 1, 2, 3,..., $\mu - 1$.

L'équation précédente revient à

$$2p = 2\Sigma a_i^2 - 2\Sigma a_i a_{i+f\omega} = \Sigma (a_i - a_{i+f\omega})^2.$$

Le second membre étant une somme de μ carrés qui s'obtiennent en posant $i = 0, 1, \ldots, \mu - 1$. En donnant à f différentes valeurs, on aura des décompositions généralement égales deux à deux.

Pour le cas de μ pair dans une décomposition, les carrés peuvent devenir égaux 2 à 2; alors on a la décomposition de p en $\frac{\mu}{2}$ carrés: cela arrive pour μ divisible par 4.

Quand on partira de l'équation

$$p = S\alpha^{\text{ind } s.s+1} . S\alpha^{-\text{ind } s.s+1},$$

qui suppose $m = 1$, $n = -2$. Si μ est impair, on aura $\omega = 1$; si μ est pair, $\omega = 2$. De là les formules :

$$2p = \Sigma (a_i - a_{i+f})^2, \quad 2p = \Sigma (a_i - a_{i+2f})^2.$$

Ainsi pour μ impair et $f = 1$, on a

$$2p = (a_0 - a_1)^2 + (a_1 - a_2)^2 + \ldots + (a_{\mu-1} - a_0)^2;$$

pour $\mu = 3$, en doublant, on aurait

$$4p = (a_1 - 2a_2 + a_0)^2 + 3(a_0 - a_1)^2.$$

Comme

$$(a_0 - a_1) + (a_1 - a_2) + (a_2 - a_0) = 0,$$

l'une des trois différences est divisible par 3. Soit $a_0 - a_1$, on aura

$$4p = (a_1 - 2a_2 + a_0)^2 + 27\left(\frac{a_0 - a_1}{3}\right)^2,$$

formule de Jacobi.

Pour $\mu = 4\mu_1$, $f = 2\mu_1$, on trouverait, les carrés étant égaux, 2 à 2,

$$p = (a_0 - a_{2\mu_1})^2 + (a_1 - a_{2\mu_1+1})^2 \ldots + (a_{2\mu_1-1} - a_{4\mu_1-1})^2.$$

Pour $\mu_1 = 1$, on a l'équation de M. Eisenstein,

$$p = (a_0 - a_2)^2 + (a_1 - a_3)^2,$$

qui l'a proposée à démontrer dans le tome XXVIII du *Journal* de M. Crelle. La démonstration qui précède est une conséquence des formules établies par M. Eisenstein dans son Mémoire sur la division du cercle. (*Journal* de M. Crelle, tome XXVII.)

Les formules données plus haut conduisent facilement aux équations (33), (35), (36), (37), (38) d'un Mémoire de M. Cauchy sur la théorie des nombres. (*Bulletin* de Férussac, 1829.)

Si l'on voulait des applications numériques, par exemple, pour

$$p = 61 = \mu\varpi + 1,$$

on pourrait prendre pour μ les valeurs 3, 4, 5, 6, 10, 12, 15, 20, 30, 60. Ainsi l'on aurait

$$p = 61,$$

μ_1,	a_0, a_1, a_2,...
3,	20, 24, 15,...
4,	17, 18, 12, 12,
5,	12, 15, 12, 14, 6,
6,	12, 12, 5, 8, 12, 10,
10,	6, 6, 6, 10, 4, 6, 9, 6, 4, 2,
12,	6, 8, 0, 2, 6, 4, 6, 4, 5, 6, 6, 6,

. . . . . .

De là les décompositions :

$\mu=3$, $2p = 122 = (20-24)^2 + (24-15)^2 + (15-20)^2 = 16 + 81 + 25$,

$\mu=4$, $p = 61 = (17-12)^2 + (18-12)^2 = 25 + 36$,

$\mu=5$, $2p = (12-15)^2 + (15-12)^2 + (12-14)^2 + (14-6)^2 + (6-12)^2$
$= 9 + 9 + 4 + 64 + 36$,

$2p = (12-12)^2 + (15-14)^2 + (12-6)^2 + (14-12)^2 + (6-15)^2$
$= 0 + 1 + 36 + 4 + 81$,

. . . . . .

Il serait superflu de multiplier les exemples.

Comme les nombres a_0, a_1, etc., trouvés par la règle d'Eisenstein, sont tous pairs sauf un, et que la demi-somme de deux carrés pairs, aussi bien que celle de deux carrés impairs, est une somme de deux carrés, il suit de ce qui précède que l'on a ces *théorèmes :*

1°. *Soit p un nombre premier, μ un diviseur quelconque de $p-1$, mais plus grand que 2, 2p sera toujours la somme de μ carrés.*

2°. *Pour μ impair, p sera la somme de $\mu+1$ carrés dont deux seront égaux.*

3°. *Pour μ pair, p sera la somme de μ carrés.*

4°. *Pour μ divisible par 4, p sera la somme de $\frac{\mu}{2}$ carrés.*

Il faut bien remarquer que zéro est mis au nombre des carrés pairs.