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

ANGELO GENOCCHI

Note sur les nombres complexes

Journal de mathématiques pures et appliquées 1re série, tome 19 (1854), p. 281-288.
<http://www.numdam.org/item?id=JMPA_1854_1_19__281_0>

NOTE SUR LES NOMBRES COMPLEXES;

PAR M. ANGELO GENOCCHI [*].

Soient n un nombre premier impair, r une racine imaginaire de l'équation $r^n = 1$, et considérons le nombre complexe

$$a + a_1 r + a_2 r^2 + \ldots + a_{n-1} r^{n-1}$$

formé avec des coefficients a_i entiers. Si ce nombre complexe est divisible par $1 - r$, nous pourrons représenter par

$$b_1 r + b_2 r^2 + \ldots + b_{n-1} r^{n-1}$$

le quotient, en supposant $b_1, b_2, \ldots, b_{n-1}$ entiers, et nous aurons

$$a + b_{n-1} + (a_1 - b_1) r + (a_2 - b_2 + b_1) r^2 + (a_3 - b_3 + b_2) r^3 + \ldots + (a_{n-1} - b_{n-1} + b_{n-2}) r^{n-1} = 0;$$

d'où, en vertu de l'équation irréductible

$$1 + r + r^2 + \ldots + r^{n-1} = 0,$$

on déduira

$$a + b_{n-1} = k, \quad a_1 - b_1 = k, \quad a_2 - b_2 + b_1 = k, \ldots, \quad a_{n-1} - b_{n-1} + b_{n-2} = k,$$

k étant un entier, et, par conséquent,

$$a + b_{n-1} = k, \quad b_1 = a_1 - k, \quad b_2 = a_1 + a_2 - 2k,$$
$$b_3 = a_1 + a_2 + a_3 - 3k, \ldots,$$
$$b_i = a_1 + a_2 + \ldots + a_i - ik, \ldots,$$
$$b_{n-1} = a_1 + a_2 + \ldots + a_{n-1} - (n-1)k.$$

[*] Il y a très-longtemps que cette Note m'a été adressée et qu'elle aurait dû être imprimée. L'auteur a depuis publié des recherches plus étendues sur la théorie des nombres. Je crois pourtant que le présent article peut encore aujourd'hui être mis utilement sous les yeux du lecteur. (J. LIOUVILLE.)

La première et la dernière de ces équations donnent

$$k = \frac{a + a_1 + a_2 + \ldots + a_{n-1}}{n},$$

et, k étant ainsi déterminé, les autres équations détermineront tous les coefficients b_i. On voit donc que la condition nécessaire et suffisante pour que le nombre complexe proposé soit divisible par $1 - r$, est que la somme

$$a + a_1 + \ldots + a_{n-1}$$

de ses coefficients soit divisible par n; théorème connu.

Supposons que chaque coefficient a_i soit formé d'après cette loi,

$$a_i = h\frac{i}{1} + h_1\frac{i(i+1)}{1.2} + h_2\frac{i(i+1)(i+2)}{1.2.3} + \ldots$$
$$+ h_m\frac{i(i+1)\ldots(i+m)}{1.2\ldots(m+1)} - \frac{i(i+1)\ldots(i+m+1)}{1.2\ldots(m+2)},$$

h, h_1, h_2,..., h_m étant des nombres entiers constants. On aura

$$a = 0,$$
$$a_1 + a_2 + \ldots + a_i = h\frac{i(i+1)}{1.2} + h_1\frac{i(i+1)(i+2)}{1.2.3} + \ldots$$
$$+ h_m\frac{i(i+1)\ldots(i+m+1)}{1.2\ldots(m+2)} - \frac{i(i+1)\ldots(i+m+2)}{1.2\ldots(m+3)},$$

et, en faisant $i = n - 1$, on verra que le second membre de cette équation aura tous ses termes divisibles par n tant que $m + 3$ sera $< n$: donc, si m est $< n - 3$, la somme

$$a + a_1 + a_2 + \ldots + a_{n-1}$$

sera divisible par n, et le nombre complexe

$$a + a_1 r + \ldots + a_{n-1} r^{n-1}$$

le sera par $1 - r$. De plus, les coefficients b_i du quotient suivront la même loi que les coefficients a_i, car

$$b_i = -k\frac{i}{1} + a_1 + a_2 + \ldots + a_i;$$

mais m dans b_i sera changé en $m + 1$. En traitant de même ce quo-

tient, et ainsi de suite, on verra que le nombre complexe primitif est divisible par la puissance $(1-r)^{n-m-3}$.

Prenons $m = n-4$, la formule

$$b_i = -k\frac{i}{1} + h\frac{i(i+1)}{1.2} + h_1\frac{i(i+1)(i+2)}{1.2.3} + \ldots$$
$$+ h_m\frac{i(i+1)(i+2)\ldots(i+m+1)}{1.2.3\ldots(m+2)} - \frac{i(i+1)\ldots(i+m+2)}{1.2\ldots(m+3)}$$

donne

$$b_1 + b_2 + b_3 + \ldots + b_i = -k\frac{i(i+1)}{1.2} + h\frac{i(i+1)(i+3)}{1.2.3} + \ldots$$
$$+ h_m\frac{i(i+1)\ldots(i+m+2)}{1.2\ldots(m+3)} - \frac{i(i+1)\ldots(i+m+3)}{1.2\ldots(m+4)},$$

et, par suite,

$$b_1 + b_2 + \ldots + b_{n-1} = -k\frac{(n-1)n}{1.2} + h\frac{(n-1)n(n+1)}{1.2.3} + \ldots$$
$$+ h_m\frac{(n-1)n(n+1)\ldots(n+m+1)}{1.2.3\ldots(m+3)} - \frac{(n-1)n(n+1)\ldots(n+m+2)}{1.2.3\ldots(m+4)},$$

dont tous les termes, excepté le dernier, sont divisibles par n; quant au dernier, il devient

$$-\frac{(n+1)(n+2)\ldots(n+m+2)}{1.2.3\ldots(n-2)},$$

et puisqu'on a

$$(n+1)(n+2)\ldots(n+m+2) = Qn + 1.2.3\ldots(m+2),$$

Q étant entier, et que

$$m+2 = n-2,$$

on conclut

$$b_1 + b_2 + \ldots + b_{n-1} \equiv -1 \pmod{n}.$$

On déduit de là ce théorème :

Que le nombre complexe primitif est divisible par $(1-r)^{n-m-3}$, *et que la somme des coefficients du quotient étant augmentée de l'unité est divisible par n.*

Je ferai quelques applications de ces résultats.

1°. Si l'on prend

$$a = n, \quad a_1 = a_2 = \ldots = a_{n-1} = 0,$$

il vient

$$\frac{n}{1-r} = -r - 2r^2 - 3r^3 - \ldots - (n-1)r^{n-1};$$

puis, en prenant

$$a = 0, \quad a_i = -i, \quad k = \frac{n-1}{2},$$

on a

$$\frac{n}{(1-r)^2} = (k-1)r + (2k-3)r^2 + (3k-6)r^3 + \ldots + \left[(n-1)k - \frac{n(n-1)}{1.2}\right] r^{n-1},$$

et, dans ce quotient, le coefficient de r^i est $ik - \frac{i(i+1)}{1.2}$, ce qui rentre dans la loi générale ci-dessus indiquée, pourvu qu'on suppose $m = 0$, $h = k$. En conséquence, ce dernier nombre complexe sera divisible par $(1-r)^{n-3}$, et la somme des coefficients du quotient $\frac{n}{(1-r)^{n-1}}$, étant augmentée de l'unité, sera divisible par n.

Or on a

$$n = (1-r)(1-r^2)(1-r^3)\ldots(1-r^{n-1}),$$

et, par suite,

$$\frac{n}{(1-r)^{n-1}} = 1 \cdot \frac{1-r^2}{1-r} \cdot \frac{1-r^3}{1-r} \cdots \frac{1-r^{n-1}}{1-r};$$

de plus

$$\frac{1-r^i}{1-r} = 1 + r + r^2 + \ldots + r^{i-1},$$

nombre complexe dont la somme des coefficients est i; de sorte que cette somme, dans le nombre complexe $\frac{n}{(1-r)^{n-1}}$, sera égale au produit $1.2.3\ldots(n-1)$. Il en résulte donc le théorème de Wilson, savoir, que le produit $1.2.3\ldots(n-1)$ augmenté de l'unité est divisible par n.

2°. En désignant par m un nombre entier non divisible par n, on peut changer r en r^m, et poser

$$n = (1-r^m)(1-r^{2m})\ldots(1-r^{(n-1)m}),$$

d'où

$$\frac{(1-r^m)(1-r^{2m})\ldots(1-r^{(n-1)m})}{(1-r)(1-r^2)\ldots(1-r^{n-1})} - 1 = \frac{n}{n} - 1 = 0.$$

Maintenant, si l'on regarde le premier membre de cette équation comme un nombre complexe divisible par $1-r$, on devra conclure que la somme de ses coefficients est divisible par n. Mais dans

$$\frac{1-r^{im}}{1-r^i} = 1 + r^i + r^{2i} + \ldots + r^{(m-1)i}$$

la somme des coefficients est toujours m; et, par suite, cette somme, dans le premier membre en question, est $m^{n-1}-1$. Donc $m^{n-1}-1$ est divisible par n; théorème de Fermat.

3°. Remplaçons r par r^2, $1-r^{2i}$ par $-r^i(r^i - r^{-i})$; puisqu'on a

$$(-1)^{n-1} = 1, \quad r^{\frac{n(n-1)}{2}} = r^{m\cdot\frac{n(n-1)}{2}} = 1,$$

il viendra

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

Posons

$$k = \frac{n-1}{2}, \quad \varphi(r) = \frac{(r^m - r^{-m})(r^{2m} - r^{-2m})\ldots(r^{km} - r^{-km})}{(r-r^{-1})(r^2-r^{-2})\ldots(r^k - r^{-k})};$$

évidemment

$$\varphi(r^{-1}) = \varphi(r);$$

mais, en observant que

$$(r^{-1})^i = r^{n-i}, \quad (r^{-1})^{-i} = r^{-n+i}, \quad (r^{-1})^{im} = r^{(n-i)m}, \quad (r^{-1})^{-im} = r^{-(n-i)m},$$

et

$$n - k = k + 1,$$

on aura aussi

$$\varphi(r^{-1}) = \frac{(r^{(n-1)m} - r^{-(n-1)m})(r^{(n-2)m} - r^{-(n-2)m})\ldots(r^{(k+1)m} - r^{-(k+1)m})}{(r^{n-1} - r^{-n+1})(r^{n-2} - r^{-n+2})\ldots(r^{k+1} - r^{-k-1})};$$

et de là

$$\varphi(r)\varphi(r^{-1}) = 1;$$

il s'ensuit

$$[\varphi(r)]^2 = 1, \quad \varphi(r) = \pm 1.$$

Désignons par ε cette valeur de $\varphi(r)$, dans le nombre complexe $\varphi(r) - \varepsilon$ la somme des coefficients sera divisible par n, et comme, en général, dans

$$\frac{r^{im} - r^{-im}}{r^i - r^{-i}} = r^{-i(m-1)} \cdot \frac{r^{2im} - 1}{r^{2i} - 1}$$
$$= r^{(m-1)(n-i)} \left(r^{2i(m-1)} + r^{2i(m-2)} + \ldots + r^{2i} + 1 \right)$$

la somme des coefficients est m, et que, par suite, elle est m^k dans $\varphi(r)$, on conclura que $m^k - \varepsilon$ est divisible par n. On a donc

$$\left(\frac{m}{n}\right) = \varepsilon,$$

en employant la notation de Legendre, ce qui donne la formule

$$\left(\frac{m}{n}\right) = \frac{(r^m - r^{-m})(r^{2m} - r^{-2m}) \ldots (r^{km} - r^{-km})}{(r - r^{-1})(r^2 - r^{-2}) \ldots (r^k - r^{-k})}.$$

Soit $m = 2$, et remarquons que si i est pair, on a

$$(-1)^i (r^i - r^{-i}) = r^i - r^{-i},$$

et si i est impair, on a

$$(-1)^i (r^i - r^{-i}) = r^{-i} - r^i = r^{n-i} - r^{-n+i};$$

observons de plus que, dans ce dernier cas, $n - i$ sera pair, et plus grand que k si i est $< k$. En posant successivement $i = 1, 2, 3, \ldots, k$, en multipliant entre eux les résultats, et se rappelant l'équation

$$1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2},$$

on obtiendra

$$(-1)^{\frac{k(k+1)}{2}} (r - r^{-1})(r^2 - r^{-2})(r^3 - r^{-3}) \ldots (r^k - r^{-k})$$
$$= (r^2 - r^{-2})(r^4 - r^{-4})(r^6 - r^{-6}) \ldots (r^{2k} - r^{-2k});$$

d'où, en vertu de la formule précédente, on tire

$$\left(\frac{2}{n}\right) = (-1)^{\frac{k(k+1)}{2}} = (-1)^{\frac{n^2-1}{8}}.$$

La même formule dispense de recourir au lemme de M. Gauss dans

la démonstration que M. Liouville a donnée de la loi de réciprocité de Legendre. Mais elle conduit aussi immédiatement à cette loi à l'aide d'une simple transformation, indiquée aussi par M. Liouville. En effet, soient m un nombre premier impair, q une racine imaginaire de l'équation

$$q^m = 1,$$

et faisons

$$h = \frac{m-1}{2};$$

nous aurons

$$\left(\frac{n}{m}\right) = \frac{(q^n - q^{-n})(q^{2n} - q^{-2n})\dots(q^{hn} - q^{-hn})}{(q - q^{-1})(q^2 - q^{-2})\dots(q^h - q^{-h})};$$

on a de plus, en général,

$$\frac{A^n - B^n}{A - B} = (Ar - Br^{-1})(Ar^2 - Br^{-2})\dots \times (Ar^{n-2} - Br^{-n+2})(Ar^{n-1} - Br^{-n+1}),$$

ou

$$\frac{A^n - B^n}{A - B} = (Ar - Br^{-1})(Ar^2 - Br^{-2})\dots(Ar^k - Br^{-k}) \times (Ar^{-1} - Br)(Ar^{-2} - Br^2)\dots(Ar^{-k} - Br^k),$$

et, de même,

$$\frac{A^m - B^m}{A - B} = (Aq - Bq^{-1})(Aq^2 - Bq^{-2})\dots(Aq^k - Bq^{-k}) \times (Aq^{-1} - Bq)(Aq^{-2} - Bq^2)\dots(Aq^{-k} - Bq^k).$$

En assignant à A, dans la premiere de ces deux équations, toutes les valeurs q, $q^2,\dots, q^k$, et dans la deuxième toutes les valeurs r, $r^2,\dots, r^k$; et prenant $B = A^{-1}$; puis en substituant dans les expressions de $\left(\frac{n}{m}\right)$ et $\left(\frac{m}{n}\right)$, on trouvera aisément

$$\left(\frac{m}{n}\right) = (-1)^{hk}\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{m}\right).$$

J'indiquerai une autre forme qu'on peut donner à la démonstration de M. Liouville. Soit g une racine primitive de la congruence

$$x^{n-1} \equiv 1 \pmod{n},$$

et soit

$$m \equiv g^\lambda \pmod{n},$$

λ étant $< n-1$: dans la suite $1+\lambda$, $2+\lambda$, $3+\lambda$,..., $k+\lambda$ le nombre des termes compris entre k et $2k$ sera λ si $\lambda < k$, sera $2k-\lambda$ si $\lambda > k$ Mais on aura

$$g^{k+i} \equiv -g^i, \quad g^{2k+i} \equiv g^i,$$

et, par suite,

$$r^{g^{k+i}} = r^{-g^i}, \quad r^{g^{2k+i}} = r^{g^i},$$

d'où il est facile de déduire

$$\left(r^{g^{1+\lambda}} - r^{-g^{1+\lambda}}\right)\left(r^{g^{2+\lambda}} - r^{-g^{2+\lambda}}\right)\ldots\left(r^{g^{k+\lambda}} - r^{-g^{k+\lambda}}\right)$$
$$= (-1)^\lambda \cdot \left(r^g - r^{-g}\right)\left(r^{g^2} - r^{-g^2}\right)\ldots\left(r^{g^k} - r^{-g^k}\right),$$

et comme

$$\left(\frac{m}{n}\right) = (-1)^\lambda, \quad g^{i+\lambda} \equiv mg^i \pmod{n}, \quad r^{g^{i+\lambda}} = r^{mg^i},$$

on en tirera

$$\left(\frac{m}{n}\right) = \frac{\left(r^{mg} - r^{-mg}\right)\left(r^{mg^2} - r^{-mg^2}\right)\ldots\left(r^{mg^k} - r^{-mg^k}\right)}{\left(r^g - r^{-g}\right)\left(r^{g^2} - r^{-g^2}\right)\ldots\left(r^{g^k} - r^{-g^k}\right)}.$$

On aura une formule analogue pour $\left(\frac{n}{m}\right)$ en appelant f une racine primitive de la congruence

$$x^{m-1} \equiv 1 \pmod{m},$$

et, à l'aide de décompositions semblables aux précédentes, on démontrera que

$$\Pi\left(\frac{q^{nf\alpha} - q^{-nf\alpha}}{q^{f\alpha} - q^{-f\alpha}}\right) = (-1)^{hk}\,\Pi\left(\frac{r^{mg_i\beta} - r^{-mg_i\beta}}{r^{g^\beta} - r^{-g^\beta}}\right),$$

les signes de multiplication Π s'étendant aux valeurs $1, 2, \ldots, h$ de α, et aux valeurs $1, 2, \ldots, k$ de β ; et de ces équations résultera la loi de réciprocité.

On peut aussi se servir de la formule

$$\left(\frac{n}{m}\right) = (-1)^{hk}\,\Pi\left(\frac{r^{mg_i\beta} - r^{-mg_i\beta}}{r^{g^\beta} - r^{-g^\beta}}\right),$$

qu'on obtient en élevant à la puissance h les deux membres de l'équation

$$n = (-1)^k\,\Pi\left(r^{g_i\beta} - r^{-g^\beta}\right)^2.$$