BONNES VIEILLES PAGES (2)

Nous vous proposons ci-dessous un texte de Leibniz dans lequel celui-ci donne une démonstration du théorème de Fermat. Ce texte, en latin, est resté manuscrit jusqu'à sa publication dans les *Œuvres* de Leibniz par C.I. Gerhardt. Nous avons fait suivre le texte d'une traduction en français d'Anne Michel-Pajus et donnons en introduction une vision moderne de la démonstration.

Les mathématiques du texte de Leibniz

Leibniz commence par calculer le coefficient M de $a^k b^l c^m d^n \ldots$, lorsqu'aucun des exposants k, l, m, ... n'est égal à e, dans le développement de $(a + b + c + d + \ldots)^e$ avec $k + l + m + n + \ldots = e$. Ce coefficient est le nombre de fois où apparaît $a^k b^l c^m d^n \ldots$ dans le développement du produit $(a + b + c + d + \ldots)(a + b + c + d + \ldots)\ldots$ avec e facteurs. Pour obtenir $a^k b^l c^m d^n \ldots$, il faut choisir k facteurs parmi les e facteurs où on prend le terme a, puis on choisit l facteurs parmi les $(e - k)$ restant où on choisit le terme b, etc. ; ainsi :

$$M = \binom{e}{k}\binom{e-k}{l}\binom{e-k-l}{m}\ldots$$

$$M = \frac{e(e-1)(e-2)\ldots(e-k+1)}{k!} \times \frac{(e-k)(e-k-1)\ldots(e-k-l+1)}{l!} \times \ldots$$

$$M = \frac{e!}{(k!)(l!)(m!)\ldots}$$

C'est bien ce que donne Leibniz (sans l'expliquer) pour $e = 19$, bien que la formule apparaisse différente à première vue. En fait, pour le coefficient de $a^5 b^4 c^3 d^3 e^2 f^1 g^1$, il commence par choisir 4 facteurs parmi 19 où il prend b, puis 3 parmi $19 - 4$ où il prend c, puis 3 parmi $19 - 4 - 3$ où il prend d, puis 2 parmi les restants où il prend e, enfin 1 avec f et 1 avec g ; dans les 5 derniers, pas de choix possible : on prend a. D'où le coefficient :

$$M = \binom{19}{4}\binom{19-4}{3}\binom{19-4-3}{3}\binom{19-4-3-3}{2}\binom{19-4-3-3-2}{1}\binom{19-4-3-3-2-1}{1}$$

$$M = \frac{19 \times (19-1) \times \ldots \times (19-13)}{4! \times 3! \times 3! \times 2! \times 1! \times 1!}.$$

On vérifie d'ailleurs aisément que :

$$M = \frac{\frac{19!}{5!}}{4! \times 3! \times 2! \times 1! \times 1!} = \frac{19!}{5! \times 4! \times 3! \times 2! \times 1! \times 1!}.$$

Leibniz affirme ensuite, toujours sans démonstration, que, lorsqu'aucun des exposants k, l, m, ... n'est égal à e, M n'est jamais premier à e. En fait, il n'utilise ce résultat que dans le cas où l'exposant e est premier ; alors e divise le facteur $M_k = \binom{e}{k}$ de M.

Si le nombre e est premier, alors e divise $(k!)M_k = e(e-1)(e-2)...$ et, comme e est premier à $(k!)$, e divise M_k (théorème de Gauss).

Si e est premier, e divise donc tous les coefficients M si aucun des exposants n'est égal à e. Donc e divise$(a + b + c + d + ...)^e - a^e - b^e - c^e$ - .... On choisit alors a = $b = c = ... = 1$; on obtient : $a^e = b^e = ...=1$ et $a + b + c + d + ... = x$ entier naturel quelconque, égal au nombre de termes choisi ; donc e divise $x^e - x$.

Portrait de Leibniz

Le texte de Leibniz (Leibniz *Mathematische Schriften* édité par Gerhardt,tome VII, Goerg Olms Verlagsbuchhanlung, Hildesheim, 1962, pp178-180)

Sed ad potestates Polynomiorum formandas redeamus, quae scilicet indigent Numeris combinatoriis, ut mox patebit. Constant autem semper ex formis ejusdem gradus, quibus numeri ex combinatoriis multiplicando formati praefiguntur. Formam voco hoc loco summam omnium membrorum ex aliquot literis similiter formatorum. Ita $a+b+c$ etc. est forma primi gradus; at formae secundi gradus sunt $a^2+b^2+c^2$ etc. et $ab+ac+bc$ etc., et formae tertii gradus sunt $a^3+b^3+c^3$ etc. et $a^2b+ab^2+a^2c+ac^2+b^2c+bc^2$ etc. et $abc+abd+bcd$ etc. Compendio autem, ut jam monui, sic designo, ut a mihi significet a vel $a+b$ vel $a+b+c$ vel etc., et $\ddot{a}$ significet a^2 vel a^2+b^2 vel $a^2+b^2+c^2$ vel etc., et $\ddot{ab}$ significet vel ab vel $ab+ac+bc$ vel $ab+ac+ad+bc+bd+cd$ vel etc., et $\dddot{a}$ erit a^3 vel a^3+b^3 vel $a^3+b^3+c^3$ vel etc., et $\dddot{a}b$ erit a^2b+ab^2 vel $a^2b+ab^2+a^2c+ac^2+b^2c+bc^2$ vel $a^2b+ab^2+a^2c+ac^2+a^2d+ad^2+b^2c+bc^2+b^2d+bd^2+c^2d+cd^2$ vel etc., et $\dddot{abc}=abc$ vel $abc+abd+bcd$ vel etc., itaque

$a+b+b$ etc. $= a$

et quadratum ab $a+b+c$ etc. $= \ddot{a}^2+2\ddot{ab}$

cubus $= \dddot{a}^3+3\dddot{a}b+6\dddot{abc}$

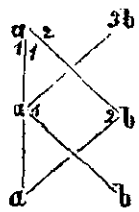
biquadratum $= \ddddot{a}^4+4\dddot{a}^3b+6\ddot{a}^2b^2+12\ddot{a}^2bc+24\ddot{abcd}$

Ut jam investigemus numeros coefficientes formis praescriptos, consideremus tot modis prodire quodvis formae membrum in potestate, quot transpositiones literarum in eo membro dari possunt; ita in cubo ab $a+b$ formae a^2b+ab^2 membrum, ut a^2b, prodit ter, quia tres ejus transpositiones seu conflationes; sic in biquadrato ipsius a^2b^2 formationes sunt sex, et in cubo de $a+b+c$ ipsius abc transpositiones sunt sex

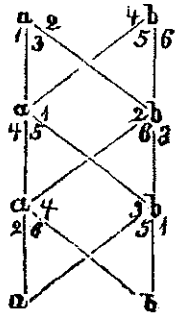
1	aab	1	aabb	1	abc
2	aba	2	abab	2	acb
3	baa	3	abba	3	bac
		4	baab	4	bca
		5	baba	5	cab
		6	bbaa	6	cba

Id lineis ductis numeros eosdem ascriptos habentibus sic apparebit:

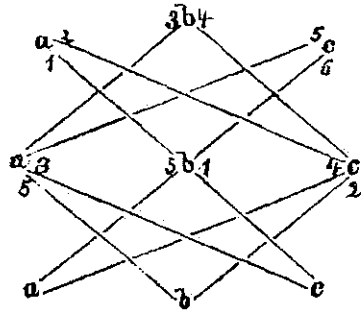
pro aab



pro aabb



pro abc



Quot vero sint transpositiones literarum Formae, nondum quod sciam determinatum extat, cum tamen inter primaria sit problemata Combinatoriae Artis. Id aliquando cum potestatibus polynomiorum aliisque hujusmodi in navi per otium sum consecutus. Multo post Cl. Joh. Bernoullius me admonente hanc eandem quam nunc dabo regulam, etsi paulo aliter expressam invenit. Igitur in exemplum, quod sit regulae intelligendae sufficiens, esto forma $a^5b^4c^3d^3e^2f^1g^1$, quaeritur quot modis ejus elementa transponi possint. Est autem gradus $5+4+3+3+2+1+1$ seu decimi noni. Dico numerum transpositionum esse proditurum, si multiplicentur invicem continue numeri Combinatorii (supra expositi) qui designant quot sint 19 rerum 4niones, 19—4 rerum 3niones, 19—4—3 rerum 3niones, 19—4—3—3 rerum 2niones, 19—4—3—3—2 rerum 1niones, 19—4—3—3—2—1 rerum 1niones. Quod etiam per productos continuorum sic poterit enuntiari, ut Numerus Transpositionum formae $a^5b^4c^3d^3e^2f^1g^1$ sit

$$\frac{19,19-1,19-2,19-3\,,,\,19-4,19-4-1,19-4-2,,}{1.2.3.4\,,,\quad 1.2.3}$$

$$\frac{19-4-3,19-4-3-1,19-4-3-2\,,,\,19-4-3-3,19-4-3-3-1,}{1.2.3\qquad\qquad 1.2}$$

$$\frac{19-4-3-3-2\,,\,19-4-3-3-2-1}{1\quad .\quad 1}.$$

Ita a^2b^2 habebit transpositiones $\frac{4,4-1\,,,4-2,4-2-1}{1.2\qquad 1.2} = \frac{4.3\,,2.1}{1.2\,,1.2} = 6.$

Porro omnis Numerus Transpositionum Formae, quem et Productum combinatoriorum appellare possis, cum alias habet proprietates memorabiles, tum hanc imprimis egregiam, ut ipse et ex-

ponens gradus, ad quem forma assurgit, non possint esse primi inter se. Unde sequitur, si exponens gradus sit numerus primitivus, necesse esse ut dividat numerum transpositionum formae in gradu, ubi tamen intelligo transpositionem quae varietatem pariat, qualis non est forma cujus elementa coincidunt ut a^2, a^3. Unde in his numerus situum non est nisi unitas. Hinc porro consequitur, ut si nomina sint numeri rationales, potestas polynomii post detractam formam invariabilem ejusdem gradus residuum relinquat, ita comparatum, ut ipsum et exponens gradus non possint esse primi inter se: et ideo cum exponens est primitivus, necessario residuum divisibile sit per exponentem. Nempe si e, item a, b, c etc., sint numeri integri et $x = a+b+c+$ etc., tunc $x^e - a^e$ et e nunquam sunt primi inter se, et ideo si e sit primitivus, erit $x^e - a^e$ divisibilis per e. Supra autem exposui, per $\ddot{a}^e$ me intelligere $a^e+b^e+c^e+$ etc. seu summam ex potestatibus omnium partium ipsi x assignatarum.

Quodsi a, b, c, sint unitates erit $a^e = a = 1$ et $\ddot{a}^e = \ddot{a} = x$, ergo $x^e - x$ et e nunquam sint primi inter se, et proinde si numerus e sit primitivus, erit $x^e - x$ divisibilis per e. Quae Numeri Primitivi proprietas Reciproca esse reperitur, ut si e non sit primitivus, etiam $x^e - x$ per e dividi non possit, sed tantum habeant aliam communem mensuram.

Traduction d'Anne Michel-Pajus

Mais revenons aux puissances des polynômes, qui ont naturellement besoin de nombres combinatoires, comme on va le voir. Elles reposent toujours sur des expressions[1] de même degré, auxquelles sont attachés des nombres formés par multiplication à partir des combinatoires. J'appelle ici expression la somme de tous les membres formés de façon semblable à partir d'un certain nombre de lettres. Ainsi a+b+c+ etc. est une expression du premier degré ; et les expressions du second degré sont $a^2+b^2+c^2$ etc. et ab+ac+bc etc. ; et les expressions du troisième degré sont $a^3+b^3+c^3$ etc. et $a^2b+ab^2+a^2c+ac^2+b^2c+bc^2$ etc. et abc+abd+bcd etc. J'abrège, comme je l'ai déjà conseillé, par cette notation : pour moi a signifie a ou a+b ou a+b+c, ou etc., $\underline{a}^2$ signifie a^2 ou a^2+b^2 ou $a^2+b^2+c^2$ ou etc., et $\underline{ab}$ signifie ab+ac+bc ou ab+ac+ad+bc+bd+cd ou etc. [...]. De sorte que

a+b+c etc. = $\underline{a}$

et le carré de a+b+c etc. = $\underline{a}^2 + 2\underline{ab}$

le cube = $\underline{a}^3+3\underline{a}^2\underline{b}+6\underline{abc}$ [...]

Comme nous avons déjà examiné les coefficients des expressions ci-dessus, nous considèrerons le nombre de façons dont se produisent les expressions des membres dans la puissance, combien de transpositions des lettres peuvent être données dans un membre. Ainsi dans le cube de a+b le membre de forme a^2b+ab^2, comme a^2b, arrive trois fois, car ses

[1] forma

transpositions ou fusions[2] sont au nombre de trois ; de même dans le bicarré du même, les formations de a^2b^2 sont au nombre de six, et dans le cube de a+b, les transpositions de abc sont au nombre de six.

1	aab	1	aabb	1	abc
2	aba	2	abab	2	acb
3	baa	3	abba	3	bac
		4	baab	4	bca
		5	baba	5	cab
		6	bbaa	6	cba

Ceci apparaîtra ainsi en traçant les lignes qui portent les mêmes nombres [voir les diagrammes sur le texte latin].

Combien il y a de transpositions de lettres d'une expression, cela n'émerge pas encore à ce que je sais, alors même que ces problèmes sont au premier rang de l'Art Combinatoire. J'ai obtenu cela dans le temps avec les puissances des polynômes et autres formes de ce genre dans l'inaction d'un voyage en bateau. Bien après la demande de l'Illustre Jean Bernouilli, je donnerai cette règle comme maintenant, même si je l'ai inventée sous une forme un peu différente. Et donc sur un exemple, ce qui est suffisant pour comprendre la règle, on demande de combien de façons les éléments de cette Expression $a^5b^4c^3d^3e^2f^1g^1$ peuvent être transposés. Son degré est 5+4+3+3+2+1+1 c'est-à-dire 19. Je dis que l'on obtiendra le nombre de transpositions, si l'on multiplie tout à tour continûment les nombres Combinatoires (exposés ci-dessus) qui désignent combien de fois il y a des quadruplets dans 19, de triplets dans 19- 4, de triplets dans 19-4-3, de couples dans 19-4-3-3, de singletons dans 19-4-3-3 –2, de singletons dans 19-4-3-3–2-1. On peut ainsi énoncer par produit de continus que le nombre de transpositions de la forme est $\frac{19,19-1,19-2,19-3,,19-4,19-4-1,19-4-2,,19-4-3,19-4-3-1,19-4-3-2}{1.2.3.4 \quad ,, \quad 1.2.3 \quad ,, \quad 1.2.3}$ *etc*

Ainsi a^2b^2 aura $\frac{4,4-1,,4-2,4-2-1}{1,2 \quad 1,2} = \frac{4.3,2.1}{1.2,1.2} = 6$ transpositions.

De plus, le nombre des transpositions de l'expression, que tu peux aussi appeler produit combinatoire, possède entre autres propriétés mémorables ce résultat exceptionnel : ce nombre et le degré auquel est élevée l'expression ne peuvent être premiers entre eux. D'où il s'ensuit que si le degré exposant est un nombre premier, il faut qu'il divise le nombre de transpositions de l'expression, où j'entends cependant une transposition qui engendre diverses formes, qui n'est pas une expression où les éléments coïncident comme a^2, a^3. Dans celles-ci le nombre de positions ne peut être que 1.

D'où il s'ensuit que [...][3] la puissance du polynôme - après retranchement de l'expression qui n'a qu'une forme à ce même degré - laisse un reste ainsi fait que lui-même et le degré exposant ne peuvent être premiers entre eux. Et bien, si e, comme a, b, c, etc. sont des nombres entiers et x = a+b+c+etc , alors $x^e - a^e$ et e ne sont jamais premiers entre eux, et donc si e est premier, $x^e - \underline{a}^e$ sera divisible par e. J'ai exposé plus haut que par $\underline{a}^e$, il faut entendre $a^e + b^e + c^e$+etc., c'est-à-dire la somme des puissances de toutes les parties de x.

Et ainsi, si les $a^e = a = 1$, l'unité, et $\underline{a}^e = \underline{a} = x$, alors $x^e - x$ et e sont premiers entre eux, et si e est premier, $x^e - x$ sera divisible par e. On a prouvé la réciproque de cette propriété du nombre premier , que si e n'est pas premier, $x^e - x$ ne peut être divisé par e, mais ils ont une commune mesure.

---

[2] Conflatio : fusion d'un métal

[3] Nous déclarons forfait pour la traduction de « si nomina sint numeri rationales ».