

Incompréhension (Denise Vella-Chemla, 10 juin 2023)

Je trouve un produit nul qui ne devrait pas l'être, selon un énoncé dans ce texte que j'ai traduit : <http://denise.vella.chemla.free.fr/trad-sommes-quad-Gauss-fr.pdf>, dans la représentation de la somme quadratique sous la forme d'un produit.

On note $\chi(k) = \left(\frac{k}{p}\right)$ et ζ une racine primitive¹ modulo p , un nombre premier. Je préfère travailler dans les corps premiers modulaires plutôt que dans les complexes (du coup, je ne vois pas ζ comme étant égale à $e^{\frac{2i\pi}{p}}$ mais plutôt comme un entier classe de congruence dans $\mathbb{Z}/p\mathbb{Z}$).

Dans l'article on trouve une expression de la somme quadratique de Gauss, qu'on note $sg(\chi)$ dans la suite, comme une somme (définition en bas de la page 2), et une autre expression de $sg(\chi)$ comme un produit (voir (1) page 6).

On doit avoir

$$sg(\chi) = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k$$

$$\text{et } (sg(\chi))^2 = (-1)^{\frac{p-1}{2}} p$$

avec $sg(\chi)$ déterminée au signe près et à la fin de l'article, l'auteur réussit à lever l'indétermination sur le signe en fonction de la classe de p modulo 4 (proposition 6.4.4).

Tandis que l'expression par le produit est (oublions le ε puisqu'il va être éliminé par la suite suivant les cas) (voir (1) p. 6) :

$$sg(\chi) = \prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)})$$

On trouve la table des racines primitives des nombres, extraite de l'OEIS dans l'article wikipedia Racine primitive.

Prenons le nombre premier 7. La table des carrés, dans laquelle on entoure les résidus quadratiques, s'écrit (les résidus quadratiques sont "en quinconce" dans la table, et au nombre de $\frac{p-1}{2}$) :

$$\begin{array}{ccc} 6 & 5 & \textcircled{4} \\ \textcircled{1} & \textcircled{2} & 3 \\ \hline 1 & 4 & 2 \end{array}$$

On arrive bien à trouver ce qu'il faut côté somme :

$$+e^{\frac{2i\pi}{7}} + e^{\frac{4i\pi}{7}} - e^{\frac{6i\pi}{7}} + e^{\frac{8i\pi}{7}} - e^{\frac{10i\pi}{7}} - e^{\frac{12i\pi}{7}}$$

¹voir annexe.

qui est un peu comme si on faisait $1 + 2 - 3 + 4 - 5 - 6 = -7$ dans le corps $\mathbb{Z}/7\mathbb{Z}$ (on met le signe + au résidus quadratiques et le signe - aux non résidus).

Mais du côté du produit, si on prend comme racine primitive de 7 la plus petite d'entre elles qui est 3, on note les puissances successives de cette racine primitive :

$$\begin{array}{c|c} \zeta^1 = 3 & \zeta^{-1} = 5 \\ \zeta^2 = 2 & \zeta^{-2} = 4 \\ \zeta^3 = 6 & \zeta^{-3} = 6 \\ \zeta^4 = 4 & \zeta^{-4} = 2 \\ \zeta^5 = 5 & \zeta^{-5} = 3 \\ \zeta^6 = 1 & \zeta^{-6} = 1 \end{array}$$

Et le produit contient les facteurs $(\zeta^1 - \zeta^{-1})(\zeta^3 - \zeta^{-3})(\zeta^5 - \zeta^{-5}) = (3 - 5)(6 - 6)(5 - 3)$ et est donc nul par son second facteur.

Pour un nombre premier $4k + 1$, tel que 13, la table des carrés est (les résidus quadratiques sont en face, au nombre de $\frac{p-1}{2}$) :

⑫	11	⑩	⑨	8	7
①	2	③	④	5	6
1	4	9	3	12	10

La somme alternée par les résidus quadratiques donne

$$1 - 2 + 3 + 4 - 5 - 6 - 7 - 8 + 9 + 10 - 11 + 12 = 39 - 39 = 0.$$

Comme Gauss nous l'a appris, ce qui est vrai pour un nombre premier de la forme $4k + 1$ est vrai pour n'importe quel nombre premier de la forme $4k + 1$ en termes de résidus quadratiques, et idem pour les $4k + 3$.

Annexe : table des racines primitives des premiers nombres, source Wikipedia

Voici une table donnant les plus petites racines primitives r modulo les nombres premiers p inférieurs à 1 000 (suite [A001918](#) de l'[OEIS](#))⁴ :

p	r	p	r	p	r	p	r	p	r	p	r	p	r	p	r	p	r	p	r	p	r	p	r
2	1	47	5	109	6	191	19	269	2	353	3	439	15	523	2	617	3	709	2	811	3	907	2
3	2	53	2	113	3	193	5	271	6	359	7	443	2	541	2	619	2	719	11	821	2	911	17
5	2	59	2	127	3	197	2	277	5	367	6	449	3	547	2	631	3	727	5	823	3	919	7
7	3	61	2	131	2	199	3	281	3	373	2	457	13	557	2	641	3	733	6	827	2	929	3
11	2	67	2	137	3	211	2	283	3	379	2	461	2	563	2	643	11	739	3	829	2	937	5
13	2	71	7	139	2	223	3	293	2	383	5	463	3	569	3	647	5	743	5	839	11	941	2
17	3	73	5	149	2	227	2	307	5	389	2	467	2	571	3	653	2	751	3	853	2	947	2
19	2	79	3	151	6	229	6	311	17	397	5	479	13	577	5	659	2	757	2	857	3	953	3
23	5	83	2	157	5	233	3	313	10	401	3	487	3	587	2	661	2	761	6	859	2	967	5
29	2	89	3	163	2	239	7	317	2	409	21	491	2	593	3	673	5	769	11	863	5	971	6
31	3	97	5	167	5	241	7	331	3	419	2	499	7	599	7	677	2	773	2	877	2	977	3
37	2	101	2	173	2	251	6	337	10	421	2	503	5	601	7	683	5	787	2	881	3	983	5
41	6	103	5	179	2	257	3	347	2	431	7	509	2	607	3	691	3	797	2	883	2	991	6
43	3	107	2	181	2	263	5	349	2	433	5	521	3	613	2	701	2	809	3	887	5	997	7