Lier décomposants de Goldbach et non-résidus quadratiques

Denise Vella-Chemla

16/4/2012

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.
Dans ses Recherches Arithmétiques, Gauss définit la notion de résidu quadratique modulo un entier de la façon suivante : a est résidu quadratique de b s'il existe c tel que $a \equiv c^2 \ (mod\ b)$.
Nous allons, pour les nombres pairs n inférieurs à 100, étudier le caractère de résiduosité quadratique à n de leurs décomposants de Goldbach, ainsi que celui de leur produit. Nous utiliserons la lettre R entre parenthèses pour signifier qu'un nombre est résidu quadratique du module n considéré et la lettre N pour signifier qu'il est non-résidu quadratique du module en question.

Module	*Produit*
8	$3\ (N) \times 5\ (N) = 15 = -1\ (N)$
12	$5\ (N) \times 7\ (N) = 35 = -1\ (N)$
16	$3\ (N) \times 13\ (N) = 7\ (N)$ $5\ (N) \times 11\ (N) = 7\ (N)$ *On réapplique aux produits* $7 \times 7 = 49 = 1\ (R)$
18	$5\ (N) \times 13\ (R) = 65 = 11\ (N)$ $7\ (R) \times 11\ (N) = 77 = 5\ (N)$ *On réapplique aux produits* $11 \times 5 = 55 = 1\ (R)$
20	$3\ (N) \times 17\ (N) = 51 = 11\ (N)$ $7\ (N) \times 13\ (N) = 91 = 11\ (N)$ *On réapplique aux produits* $11 \times 11 = 121 = 1\ (R)$
24	$5\ (N) \times 19\ (N) = 95 = -1\ (N)$ $7\ (N) \times 17\ (N) = 119 = -1\ (N)$ $11\ (N) \times 13\ (N) = 143 = -1\ (N)$
28	$5\ (N) \times 23\ (N) = 115 = 3\ (N)$ $11\ (N) \times 17\ (N) = 187 = 19\ (N)$ *On réapplique aux produits* $3 \times 19 = 57 = 1\ (R)$
30	$7\ (N) \times 23\ (N) = 151 = 1\ (R)$ $11\ (N) \times 19\ (R) = 209 = 29 = -1\ (N)$ $13\ (N) \times 17\ (N) = 221 = 11\ (N)$ *On réapplique aux produits* $29 \times 11 = 19\ (R)$ $19 \times 19 = 361 = 1\ (R)$
32	$3\ (N) \times 29\ (N) = 87 = 23\ (N)$ $13\ (N) \times 19\ (N) = 247 = 23\ (N)$ *On réapplique aux produits* $23 \times 23 = 529 = 17\ (R)$ $17 \times 17 = 289 = 1\ (R)$

Module	*Produit*
36	$5\ (N) \times 31\ (N) = 155 = 11\ (N)$ $7\ (N) \times 29\ (N) = 203 = 23\ (N)$ $13\ (O) \times 23\ (N) = 299 = 11\ (N)$ $17\ (N) \times 19\ (N) = 323 = 35 = -1\ (N)$ *On réapplique aux produits* $11 \times 23 = 1$
40	$3\ (N) \times 37\ (N) = 111 = 31\ (N)$ $11\ (N) \times 29\ (N) = 319 = -1\ (N)$ $17\ (N) \times 23\ (N) = 391 = 31\ (N)$ *On réapplique aux produits* $31 \times 31 = 961 = 1\ (R)$
42	$5\ (N) \times 37\ (R) = 185 = 17\ (N)$ $11\ (N) \times 31\ (N) = 341 = 5\ (N)$ $13\ (N) \times 29\ (N) = 377 = 41 = -1\ (N)$ $19\ (N) \times 23\ (N) = 437 = 17\ (N)$ *On réapplique aux produits* $17 \times 5 = 85 = 1\ (R)$
44	$3\ (N) \times 41\ (N) = 123 = 35\ (N)$ $7\ (N) \times 37\ (R) = 259 = 39\ (N)$ $13\ (N) \times 31\ (N) = 403 = 7\ (N)$ *On réapplique aux produits* $35 \times 39 = 1365 = 1\ (R)$
48	$5\ (N) \times 43\ (N) = 215 = 23\ (N)$ $7\ (N) \times 41\ (N) = 287 = 47 = -1\ (N)$ $11\ (N) \times 37\ (N) = 407 = 23\ (N)$ $17\ (N) \times 31\ (N) = 527 = 47 = -1\ (N)$ $19\ (N) \times 29\ (N) = 551 = 23\ (N)$ *On réapplique aux produits* $23^2 = 529 = 1\ (R)$
50	$3\ (N) \times 47\ (N) = 141 = 41\ (R)$ $7\ (N) \times 43\ (N) = 301 = 1\ (R)$ $13\ (N) \times 37\ (N) = 481 = 31\ (R)$ $19\ (R) \times 31\ (R) = 589 = 39\ (R)$ *On réapplique aux produits* $41 \times 39 = 1599 = -1\ (R)$
52	$5\ (N) \times 47\ (N) = 235 = 27\ (N)$ $11\ (N) \times 41\ (N) = 451 = 35\ (N)$ $23\ (N) \times 29\ (R) = 667 = 43\ (N)$ *On réapplique aux produits* $27 \times 43 \times 43 \times 35 = 1747305 = 1\ (R)$ $27 \times 27 = 1\ (R)$
54	$7\ (R) \times 47\ (N) = 329 = 5\ (N)$ $11\ (N) \times 43\ (R) = 473 = 41\ (N)$ $13\ (R) \times 41\ (N) = 533 = 47\ (N)$ $17\ (N) \times 37\ (R) = 629 = 35\ (N)$ $23\ (N) \times 31\ (R) = 713 = 11\ (N)$ *On réapplique aux produits* $5 \times 11 = 1\ (R)$ $41 \times 47 \times 35 = -1\ (R)$
56	$3\ (N) \times 53\ (N) = 159 = 47\ (N)$ $13\ (N) \times 43\ (N) = 559 = -1\ (N)$ $19\ (N) \times 37\ (N) = 703 = 31\ (N)$ *On réapplique aux produits* $47 \times 31 = 1\ (R)$

Module	*Produit*
60	$7\ (N) \times 53\ (N) = 371 = 11\ (N)$ $13\ (N) \times 47\ (N) = 611 = 11\ (N)$ $17\ (N) \times 43\ (N) = 731 = 11\ (N)$ $19\ (N) \times 41\ (N) = 779 = -1\ (N)$ $23\ (N) \times 37\ (N) = 851 = 11\ (N)$ $29\ (N) \times 31\ (N) = 899 = -1\ (N)$ *On réapplique aux produits* $11^2 = 1\ (R)$
64	$3\ (N) \times 61\ (N) = 183 = 55\ (N)$ $5\ (N) \times 59\ (N) = 295 = 39\ (N)$ $11\ (N) \times 53\ (N) = 583 = 7\ (N)$ $17\ (R) \times 47\ (N) = 799 = 31\ (N)$ $23\ (N) \times 41\ (R) = 943 = 47\ (N)$ *On réapplique aux produits* $31^2 = 1\ (R)$ $47^4 = 1\ (R)$ $55 \times 7 = 385 = 1\ (R)$ $39 \times 39 \times 47 = 71487 = -1\ (N)$
66	$5\ (N) \times 61\ (N) = 305 = 41\ (N)$ $7\ (N) \times 59\ (N) = 413 = 17\ (N)$ $13\ (N) \times 53\ (N) = 689 = 29\ (N)$ $19\ (N) \times 47\ (N) = 893 = 35\ (N)$ $23\ (N) \times 43\ (N) = 989 = 65\ (N)$ $29\ (N) \times 37\ (R) = 1073 = 17\ (N)$ *On réapplique aux produits* $41 \times 29 = 1189 = 1\ (R)$ $17 \times 35 = 595 = 1\ (R)$
68	$7\ (N) \times 61\ (N) = 427 = 19\ (N)$ $31\ (N) \times 37\ (N) = 1147 = 59\ (N)$ *On réapplique aux produits* $19^2 \times 59^2 = 1256641 = 1\ (R)$
70	$3\ (N) \times 67\ (N) = 201 = 61\ (N)$ $11\ (R) \times 59\ (N) = 649 = 19\ (N)$ $17\ (N) \times 53\ (N) = 901 = 61\ (N)$ $23\ (N) \times 47\ (N) = 1081 = 31\ (N)$ $29\ (R) \times 41\ (N) = 1189 = -1\ (N)$ *On réapplique aux produits* $61 \times 31 = 1891 = 1\ (R)$
72	$5\ (N) \times 67\ (N) = 335 = 47\ (N)$ $11\ (N) \times 61\ (N) = 671 = 23\ (N)$ $13\ (N) \times 59\ (N) = 767 = 47\ (N)$ $19\ (N) \times 53\ (N) = 1007 = -1\ (N)$ $29\ (N) \times 43\ (N) = 1247 = 23\ (N)$ $31\ (N) \times 41\ (N) = 1271 = 47\ (N)$ *On réapplique aux produits* $47^2 \times 23^2 = 1168561 = 1\ (R)$
76	$3\ (N) \times 73\ (R) = 219 = 67\ (N)$ $5\ (N) \times 71\ (N) = 355 = 51\ (N)$ $17\ (N) \times 59\ (N) = 1003 = 15\ (N)$ $23\ (N) \times 53\ (N) = 1219 = 3\ (N)$ $29\ (N) \times 47\ (N) = 1363 = 71\ (N)$ *On réapplique aux produits* $51 \times 3 = 153 = 1\ (R)$ $15 \times 71 = 1065 = 1\ (R)$

Module	*Produit*
78	$5\ (N) \times 73\ (N) = 365 = 53\ (N)$ $7\ (N) \times 71\ (N) = 497 = 29\ (N)$ $11\ (N) \times 67\ (N) = 737 = 35\ (N)$ $17\ (N) \times 61\ (R) = 1037 = 23\ (N)$ $19\ (N) \times 59\ (N) = 1121 = 29\ (N)$ $31\ (N) \times 47\ (N) = 1457 = 53\ (N)$ $37\ (N) \times 41\ (N) = 1517 = 35\ (N)$ *On réapplique aux produits* $53^2 = 2809 = 1\ (R)$ $29 \times 35 = 1015 = 1\ (R)$ $23^3 = 12167 = -1\ (N)$
80	$7\ (N) \times 73\ (N) = 511 = 31\ (N)$ $13\ (N) \times 67\ (N) = 871 = 71\ (N)$ $19\ (N) \times 61\ (N) = 1159 = 39\ (N)$ $37\ (N) \times 43\ (N) = 1591 = 71\ (N)$ *On réapplique aux produits* $31^2 = 961 = 1\ (R)$ $39^2 = 1521 = 1\ (R)$ $71^2 = 5041 = 1\ (R)$
84	$5\ (N) \times 79\ (N) = 395 = 59\ (N)$ $11\ (N) \times 73\ (N) = 803 = 47\ (N)$ $13\ (N) \times 71\ (N) = 923 = -1\ (N)$ $17\ (N) \times 67\ (N) = 1139 = 47\ (N)$ $23\ (N) \times 61\ (N) = 1403 = 59\ (N)$ $31\ (N) \times 53\ (R) = 1643 = 47\ (N)$ $37\ (R) \times 47\ (N) = 1739 = 59\ (N)$ $41\ (N) \times 43\ (R) = 1763 = -1\ (N)$ *On réapplique aux produits* $47 \times 59 = 2773 = 1\ (R)$
88	$5\ (N) \times 83\ (N) = 415 = 63\ (N)$ $17\ (N) \times 71\ (N) = 1207 = 63\ (N)$ $29\ (N) \times 59\ (N) = 1711 = 39\ (N)$ $41\ (N) \times 47\ (N) = 1927 = 79\ (N)$ *On réapplique aux produits* $39 \times 79 = 3081 = 1\ (R)$
90	$7\ (N) \times 83\ (N) = 581 = 41\ (N)$ $11\ (N) \times 79\ (R) = 869 = 59\ (N)$ $17\ (N) \times 73\ (N) = 1241 = 71\ (N)$ $19\ (R) \times 71\ (N) = 1349 = -1\ (N)$ $23\ (N) \times 67\ (N) = 1541 = 11\ (N)$ $29\ (N) \times 61\ (R) = 1769 = 59\ (N)$ $31\ (R) \times 59\ (N) = 1829 = 29\ (N)$ $37\ (N) \times 53\ (N) = 1961 = 71\ (N)$ $43\ (N) \times 47\ (N) = 2021 = 41\ (N)$ *On réapplique aux produits* $41 \times 11 = 451 = 1\ (R)$ $59 \times 29 = 1711 = 1\ (R)$ $71^2 = 5041 = 1\ (R)$
92	$3\ (N) \times 89\ (N) = 267 = 83\ (N)$ $13\ (R) \times 79\ (N) = 1027 = 15\ (N)$ $19\ (N) \times 73\ (R) = 1387 = 7\ (N)$ $31\ (N) \times 61\ (N) = 1891 = 51\ (N)$ *On réapplique aux produits* $83 \times 51 = 4233 = 1\ (R)$

Module	*Produit*
96	$7\ (N) \times 89\ (N) = 623 = 47\ (N)$ $13\ (N) \times 83\ (N) = 1079 = 23\ (N)$ $17\ (N) \times 79\ (N) = 1343 = 95 = -1\ (N)$ $23\ (N) \times 73\ (R) = 1679 = 47\ (N)$ $29\ (N) \times 67\ (N) = 1943 = 23\ (N)$ $37\ (N) \times 59\ (N) = 2183 = 71\ (N)$ $43\ (N) \times 53\ (N) = 2279 = 71\ (N)$ *On réapplique aux produits* $47^2 = 1\ (R)$ $23 \times 71 = 1\ (R)$
98	$19\ (N) \times 79\ (R) = 1501 = 31\ (N)$ $31\ (N) \times 67\ (R) = 2077 = 19\ (N)$ $37\ (R) \times 61\ (N) = 2257 = 3\ (N)$ *On réapplique aux produits* $31 \times 19 = 1\ (R)$
100	$3\ (N) \times 97\ (N) = 291 = 91\ (N)$ $11\ (N) \times 89\ (R) = 979 = 79\ (N)$ $17\ (N) \times 83\ (N) = 1411 = 11\ (N)$ $29\ (R) \times 71\ (N) = 2059 = 59\ (N)$ $41\ (R) \times 59\ (N) = 2419 = 19\ (N)$ $47\ (N) \times 53\ (N) = 2491 = 91\ (N)$ *On réapplique aux produits* $91 \times 11 = 1\ (R)$ $79 \times 19 = 1\ (R)$ $59^5 = -1\ (N)$

Le problème auquel on est confronté, c'est que si on étudie maintenant les produits pour les nombres premiers impairs qui ne sont pas des décomposants de Goldbach de n, rien ne semble les distinguer des décomposants. Par exemple, pour le nombre pair 100, on obtient pour les produits des non-décomposants de Goldbach :

Module	*Produit*
100	$7\ (N) \times 93\ (N) = 651 = 51\ (N)$ $13\ (N) \times 87\ (N) = 1131 = 31\ (N)$ $19\ (N) \times 81\ (R) = 1539 = 39\ (N)$ $23\ (N) \times 77\ (N) = 1771 = 71\ (N)$ $31\ (N) \times 69\ (R) = 2179 = 79\ (N)$ $37\ (N) \times 63\ (N) = 2331 = 31\ (N)$ *On réapplique aux produits* $31 \times 71 = 1\ (R)$ $51^2 = 1\ (R)$ $39^5 = -1\ (N)$ $79^5 = -1\ (N)$

Annexe 1 : Groupe des unités

Un décomposant de Goldbach de n, s'il existe, est un élément du groupe des unités $(\mathbb{Z}/n\mathbb{Z})^*$. Son complémentaire à n appartient lui aussi au groupe des unités. Le groupe des unités forme un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, \times)$. Son ordre divise l'ordre du groupe en question.

Annexe 2 : Journal mathématique de Gauss

On lit dans le journal mathématique de Gauss qu'il s'est intéressé à la conjecture de Goldbach en date du 14 mai 1796. Les traducteurs du journal en français, P. Eymard et J.P. Lafon, écrivent en préface à leur traduction : *"à plusieurs reprises, nous voyons Gauss découvrir d'importants théorèmes par des essais numériques et provoquer l'heureuse rencontre des chiffres, forçant ensuite la démonstration rigoureuse par une recherche de plusieurs mois"*.
Gauss écrit également en date du 9 juillet 1814 : *"Dedekind a de cette manière vérifié la proposition pour tous les nombres premiers inférieurs à 100"*.
Cependant, Henri Poincaré écrit dans la Science et l'Hypothèse : *"une accumulation de faits n'est pas plus une science qu'un tas de pierres n'est une maison"*.

Annexe 3 : articles 101 et 106 des Recherches Arithmétiques

Article 101 : Tout nombre non-divisible par p, qui est résidu de p sera aussi résidu de p^n ; celui qui ne sera pas résidu de p ne le sera pas non plus de p^n.

Article 106 : On voit de ce qui précède, qu'il suffit de reconnaître si un nombre donné est résidu ou non-résidu d'un nombre premier donné, et que tous les cas reviennent à celui-là.
Un nombre quelconque A, non-divisible par un nombre premier $2m + 1$, est résidu ou non-résidu de ce nombre premier suivant que $A^m \equiv +1$ *ou* $\equiv -1$ $(mod\ 2m + 1)$.

Annexe 4 : Nombre de résidus quadratiques d'un module quelconque

Les formules suivantes, fournies par M. Banderier, permettent de calculer le nombre de résidus quadratiques (noté $\rho_2(n)$) du module n :

- $\rho_2(2) = 2$
- $\rho_2(p) = \dfrac{p+1}{2}$
- $\rho_2(2^n) = \dfrac{3}{2} + \dfrac{2^n}{6} + \dfrac{(-1)^{n+1}}{6}$
- $\rho_2(p^n) = \dfrac{3}{4} + \dfrac{(p-1)(-1)^{n+1}}{4(p+1)} + \dfrac{p^{n+1}}{2(p+1)}$
- $\rho_2(mn) = \rho_2(m)\rho_2(n)$.