Pourquoi tout nombre pair sauf 2 est-il la somme de deux nombres premiers ?

Denise Vella-Chemla

5/10/11

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.
Cette conjecture est trivialement vérifiée par les nombres pairs doubles de nombres premiers.
On rappelle que p est un décomposant de Goldbach de n si p est un nombre premier incongru[1] à n selon tout module premier inférieur à $\sqrt{n}$.

$$\forall\, n \geq 6,\ \ n\ =\ p+q,\ p\ et\ q\ premiers\ impairs \iff \forall\, q \leq \sqrt{n},\quad p \not\equiv n\ (q)^2$$

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. Il y a $\varphi(n)$ décompositions possibles qui font intervenir deux unités complémentaires (on les a notées en annexe 2 dans chacune des colonnes de tables que l'on fournit pour les nombres pairs de 8 à 100). Le groupe des unités forme un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, \times)$. Son ordre divise l'ordre du groupe en question. Il y a donc au plus $\varphi(n)/2$ décompositions qui sont constituées de deux sommants qui sont tous les deux des unités. Par le principe des tiroirs, cela entraîne dans la plupart des cas qu'il y a au plus un résidu quadratique par colonne (ou inversement, au moins un non-résidu par colonne) ; remarque : cela n'est pas le cas lorsque les résidus quadratiques sont *"en face"* (cf par exemple la table en annexe d'un nombre de la forme $2.(4n+3)^2$ comme 50). Dans la plupart des cas donc, une décomposition de Goldbach a l'un de ses deux sommants qui est un non-résidu quadratique. Le carré de ce non-résidu est un résidu puisque le produit de deux non-résidus est un résidu. Un tel nombre est donc à chercher, s'il existe, parmi les racines carrés des résidus quadratiques inversibles de n (en annexe 1, sont fournies les racines carrées des résidus quadratiques inversibles de n pour n compris entre 2 et 100).

Il reste à comprendre, et c'est là l'essentiel, pourquoi l'une des racines carrées en question est forcément incongrue à n selon tous les nombres premiers impairs inférieurs à $\sqrt{n}$.

[1] On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.
[2] Par exemple, 98 a pour plus petit décomposant de Goldbach 19 parce que 3, 5, 7, 11, 13 et 17 sont tous congrus à 98 selon "quelqu'un".

$$98 = 2.7^2.$$
$$98 \equiv 3\ (mod\ 5).$$
$$98 \equiv 5\ (mod\ 3).$$
$$98 \equiv 7\ (mod\ 7).$$
$$98 \equiv 11\ (mod\ 3).$$
$$98 \equiv 13\ (mod\ 5).$$
$$98 \equiv 17\ (mod\ 3).$$

Annexe 1 : Résidus quadratiques inversibles de n et leur racine carrée

2 : 1 (1)
4 : 1 (3)
6 : 1 (5)
8 : 1 (7)
10 : 1 (9) 9 (7)
12 : 1 (11)
14 : 1 (13) 9 (11) 11 (9)
16 : 1 (15) 9 (13)
18 : 1 (17) 7 (13) 13 (11)
20 : 1 (19) 9 (17)
22 : 1 (21) 3 (17) 5 (15) 9 (19) 15 (13)
24 : 1 (23)
26 : 1 (25) 3 (17) 9 (23) 17 (15) 23 (19) 25 (21)
28 : 1 (27) 9 (25) 25 (23)
30 : 1 (29) 19 (23)
32 : 1 (31) 9 (29) 17 (25) 25 (27)
34 : 1 (33) 9 (31) 13 (25) 15 (27) 19 (23) 21 (19) 25 (29) 33 (21)
36 : 1 (35) 13 (29) 25 (31)
38 : 1 (37) 5 (29) 7 (27) 9 (35) 11 (31) 17 (25) 23 (21) 25 (33) 35 (23)
40 : 1 (39) 9 (37)
42 : 1 (41) 25 (37) 37 (31)
44 : 1 (43) 5 (37) 9 (41) 25 (39) 37 (35)
46 : 1 (45) 3 (39) 9 (43) 13 (29) 25 (41) 27 (25) 29 (35) 31 (33) 35 (37) 39 (27) 41 (31)
48 : 1 (47) 25 (43)
50 : 1 (49) 9 (47) 11 (31) 19 (37) 21 (39) 29 (27) 31 (41) 39 (33) 41 (29) 49 (43)
52 : 1 (51) 9 (49) 17 (41) 25 (47) 29 (43) 49 (45)
54 : 1 (53) 7 (41) 13 (43) 19 (37) 25 (49) 31 (29) 37 (35) 43 (31) 49 (47)
56 : 1 (55) 9 (53) 25 (51)
58 : 1 (57) 5 (47) 7 (35) 9 (55) 13 (39) 23 (49) 25 (53) 33 (31) 35 (37) 45 (33) 49 (51)
51 (43) 53 (45) 57 (41)
60 : 1 (59) 49 (53)
62 : 1 (61) 5 (37) 7 (41) 9 (59) 19 (53) 25 (57) 33 (39) 35 (33) 39 (47) 41 (45) 45 (49) 47 (35)
49 (55) 51 (43) 59 (51)
64 : 1 (63) 9 (61) 17 (55) 25 (59) 33 (49) 41 (51) 49 (57) 57 (53)
66 : 1 (65) 25 (61) 31 (47) 37 (53) 49 (59)
68 : 1 (67) 9 (65) 13 (59) 21 (53) 25 (63) 33 (55) 49 (61) 53 (57)
70 : 1 (69) 9 (67) 11 (61) 29 (57) 39 (47) 51 (59)
72 : 1 (71) 25 (67) 49 (65)
74 : 1 (73) 3 (59) 7 (65) 9 (71) 11 (51) 21 (61) 25 (69) 27 (45) 33 (49) 41 (39) 47 (63) 49 (67)
53 (41) 63 (47) 65 (55) 67 (57) 71 (53) 73 (43)
76 : 1 (75) 5 (67) 9 (73) 17 (63) 25 (71) 45 (65) 49 (69) 61 (59) 73 (61)
78 : 1 (77) 25 (73) 43 (67) 49 (71) 55 (61) 61 (55)
80 : 1 (79) 9 (77) 41 (69) 49 (73)
82 : 1 (81) 5 (69) 9 (79) 21 (53) 23 (49) 25 (77) 31 (61) 33 (63) 37 (59) 39 (71) 43 (65) 45 (43)
49 (75) 51 (57) 57 (45) 59 (51) 61 (67) 73 (55) 77 (47) 81 (73)
84 : 1 (83) 25 (79) 37 (73)
86 : 1 (85) 9 (83) 11 (65) 13 (63) 15 (55) 17 (67) 21 (51) 23 (61) 25 (81) 31 (69) 35 (75) 41 (59)
47 (45) 49 (79) 53 (71) 57 (53) 59 (47) 67 (57) 79 (49) 81 (77) 83 (73)
88 : 1 (87) 9 (85) 25 (83) 49 (81) 81 (79)
90 : 1 (89) 19 (73) 31 (79) 49 (83) 61 (59) 79 (77)

92 : 1 (91) 9 (89) 13 (75) 25 (87) 29 (81) 41 (77) 49 (85) 73 (71) 77 (79) 81 (83) 85 (73)
94 : 1 (93) 3 (59) 7 (77) 9 (91) 17 (55) 21 (63) 25 (89) 27 (83) 37 (79) 49 (87) 51 (49)
53 (57) 55 (61) 59 (71) 61 (69) 63 (51) 65 (73) 71 (67) 75 (81) 79 (75) 81 (85) 83 (53) 89 (65)
96 : 1 (95) 25 (91) 49 (89) 73 (83)
98 : 1 (97) 9 (95) 11 (65) 15 (57) 23 (87) 25 (93) 29 (83) 37 (73) 39(75) 43(71) 51(59)
53(51) 57(69) 65(53) 67(79) 71(85) 79(67) 81(89) 85(55) 93(81) 95(61)
100 : 1 (99) 9 (97) 21 (89) 29 (77) 41 (79) 49 (93) 61 (81) 69 (87) 81 (91) 89 (83)

Annexe 2 : tables des inversibles $(\mathbb{Z}/n\mathbb{Z})^*$ fournissant les résidus quadratiques et les décompositions de Goldbach de n

Dans les tables suivantes, seules sont fournies les décompositions mettant en jeu par colonne deux unités du groupe $(\mathbb{Z}/n\mathbb{Z})^*$. Les décompositions de Goldbach sont marquées d'une croix. Les résidus quadratiques de n sont colorés en bleu. Remarque : comme Cantor, on considèrera que la décomposition $1 + (n-1)$ est une décomposition de Goldbach lorsque $n-1$ est premier.

A2.1 : Nombres pairs doubles d'impairs non premiers

Selon les modules qui sont des nombres pairs doubles d'impairs non-premiers (les $4n+2$ qui ne sont pas doubles d'un nombre premier impair), $x\ R\ 2p \iff x+p\ R\ 2p$.

Selon le module $18 = 2.3^2$, de la forme $2(4n+3)^2$:

17	13	11
1	5	7
	×	×

Selon le module $30 = 2p = 2.3.5$, de la forme $2(4n+3)(4n+1)$:

29	23	19	17
1	7	11	13
	×	×	×

Selon le module $42 = 2.3.7$, de la forme $2(4n+3)(4n'+3)$:

41	37	31	29	25	23
1	5	11	13	17	19
×	×	×	×		×

Selon le module $50 = 2.5^2$, de la forme $2(4n+1)^2$:

49	47	43	41	39	37	33	31	29	27
1	3	7	9	11	13	17	19	21	23
	×	×			×		×		

Selon le module $54 = 2.3^3$, de la forme $2(4n+3)^3$:

53	49	47	43	41	37	35	31	29
1	5	7	11	13	17	19	23	25
×		×	×	×	×		×	

Selon le module $66 = 2.3.11$, de la forme $2(4n+3)(4n'+3)$:

65	61	59	53	49	47	43	41	37	35
1	5	7	13	17	19	23	25	29	31
	×	×	×		×	×		×	

Selon le module $70 = 2.5.7$, de la forme $2(4n+1)(4n'+3)$:

69	67	61	59	57	53	51	47	43	41	39	37
1	3	9	11	13	17	19	23	27	29	31	33
	×		×		×		×		×		

Selon le module $78 = 2.3.13$, de la forme $2(4n+3)(4n'+1)$:

77	73	71	67	61	59	55	53	49	47	43	41
1	5	7	11	17	19	23	25	29	31	35	37
	×	×	×	×	×				×		×

Selon le module $90 = 2.3^2.5$, de la forme $2(4n+3)^2(4n'+1)$:

89	83	79	77	73	71	67	61	59	53	49	47
1	7	11	13	17	19	23	29	31	37	41	43
×	×	×		×	×	×	×	×	×		×

Selon le module $98 = 2.7^2$, de la forme $2(4n+3)^2$:

97	95	93	89	87	85	83	81	79	75	73	71	69	67	65	61	59	57	55	53	51
1	3	5	9	11	13	15	17	19	23	25	27	29	31	33	37	39	41	43	45	47
×								×					×		×					

On peut démontrer que x et $x+p$ ont le même caractère de résiduosité à n.

A2.2 : Nombres pairs doubles de pairs

Pour les nombres pairs doubles de pairs, on constate parfois des symétries telles que l'on a deux décompositions de Goldbach possibles, symétriques l'une de l'autre par rapport au milieu des tables.

Selon le module 8, de la forme 2^3 :

7	5
1	3
×	×

Selon le module $12 = 2^2.3$, de la forme $4(4n+3)$:

11	7
1	5
×	×

Selon le module 16, de la forme 2^4 :

15	13	11	9
1	3	5	7
	×	×	

Selon le module $20 = 2^2.5$, de la forme $4(4n+1)$:

19	17	13	11
1	3	7	9
×	×	×	

Selon le module $24 = 2^3.3$, de la forme $2^3(4n+3)$:

23	19	17	13
1	5	7	11
×	×	×	×

Selon le module $28 = 2^2.7$, de la forme $4(4n+3)$:

27	25	23	19	17	15
1	3	5	9	11	13
		×		×	

Selon le module 32, de la forme 2^5 :

31	29	27	25	23	21	19	17
1	3	5	7	9	11	13	15
×	×					×	

Selon le module $36 = 2^2.3^2$, de la forme $4(4n+3)^2$:

35	31	29	25	23	19
1	5	7	11	13	17
	×	×		×	×

Selon le module $40 = 2^4.5$, de la forme $2^4(4n+1)$:

39	37	33	31	29	27	23	21
1	3	7	9	11	13	17	19
	×			×		×	

Selon le module $44 = 2^2.11$, de la forme $4(4n+3)$:

43	41	39	37	35	31	29	27	25	23
1	3	5	7	9	13	15	17	19	21
×	×		×		×				

Selon le module $48 = 2^4.3$, de la forme $2^4(4n+3)$:

47	43	41	37	35	31	29	25
1	5	7	11	13	17	19	23
	×	×	×		×	×	

Selon le module $52 = 2^2.13$, de la forme $4(4n+1)$:

51	49	47	45	4	41	37	35	33	31	29	27
1	3	5	7	9	11	15	17	19	21	23	25
		×			×					×	

Selon le module $56 = 2^3.7$, de la forme $2^3(4n+3)$:

55	53	51	47	45	43	41	39	37	33	31	29
1	3	5	9	11	13	15	17	19	23	25	27
	×				×			×			

Selon le module $60 = 2^2.3.5$, de la forme $4(4n+3)(4n'+1)$:

59	53	49	47	43	41	37	31
1	7	11	13	17	19	23	29
×	×		×	×	×	×	×

Selon le module 64, de la forme 2^6 :

63	61	59	57	55	53	51	49	47	45	43	41	39	37	35	33
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
	×	×			×			×			×				

Selon le module $68 = 2^2.17$, de la forme $4(4n+1)$:

67	65	63	61	59	57	55	53	49	47	45	43	41	39	37	35
1	3	5	7	9	11	13	15	19	21	23	25	27	29	31	33
×			×											×	

Selon le module $72 = 2^3.3^2$, de la forme $2^3(4n+3)^2$:

71	67	65	61	59	55	53	49	47	43	41	37
1	5	7	11	13	17	19	23	25	29	31	35
×	×		×	×		×			×	×	

Selon le module $76 = 2^2.19$, de la forme $4(4n+3)$:

75	73	71	69	67	65	63	61	59	55	53	51	49	47	45	43	41	39
1	3	5	7	9	11	13	15	17	21	23	25	27	29	31	33	35	37
	×	×						×		×			×				

Selon le module $80 = 2^4.5$, de la forme $2^4(4n+1)$:

79	77	73	71	69	67	63	61	59	57	53	51	49	47	43	41
1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39
×		×			×		×							×	

Selon le module $84 = 2^2.3.7$, de la forme $4(4n+3)(4n'+3)$:

83	79	73	71	67	65	61	59	55	53	47	43
1	5	11	13	17	19	23	25	29	31	37	41
×	×	×	×	×		×			×	×	×

Selon le module $88 = 2^3.11$, de la forme $2^3(4n+3)$:

87	85	83	81	79	75	73	71	69	67	65	61	59	57	55	53	51	47	45
1	3	5	7	9	13	15	17	19	23	25	27	29	31	33	37	39	41	43
		×					×					×					×	

Selon le module $92 = 2^2.23$, de la forme $4(4n+3)$:

91	89	87	85	83	81	79	77	75	73	71	67	65	63	61	59	57	55	53	51	49	47
1	3	5	7	9	11	13	15	17	19	21	25	27	29	31	33	35	37	39	41	43	45
	×					×			×					×							

Selon le module $96 = 2^5.3$, de la forme $2^5(4n+3)$:

95	91	89	85	83	79	77	73	71	67	65	61	59	55	53	49
1	5	7	11	13	17	19	23	25	29	31	35	37	41	43	47
		×		×	×		×		×			×		×	

Selon le module $100 = 2^2.5^2$, de la forme $4(4n+1)^2$:

99	97	93	91	89	87	83	81	79	77	73	71	69	67	63	61	59	57	53	51
1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39	41	43	47	49
	×			×		×					×					×		×	