Montrer ce qu'on a trouvé, même si on ne sait rien démontrer (Denise Vella-Chemla, 1.8.18)

A la recherche d'une inatteignable démonstration de la conjecture de Goldbach [*], voici ce qu'on a trouvé récemment : on sait qu'un décomposant de Goldbach d'un nombre n est premier à n (puisqu'il est premier tout court). Quand on calcule les restes des divisions de $p(n-p) = -p^2$ par n, on réalise que l'un des décomposants de Goldbach de n [†] a systématiquement le reste de la division de l'opposé de son carré par n qui est premier.

Ci-dessous, les tables de multiplication modulaire selon n jusqu'à 60 dans lesquelles on ne note que les restes des divisions par n qui sont premiers. Les décompositions de Goldbach de n sont colorées en bleu sur la diagonale ascendante. On peut noter le rétrécissement des tables pour les pairs multiples de 3. Dans chaque ligne et chaque colonne apparaissent tous les nombres premiers inférieurs à n qui ne divisent pas n une fois et une seule chacun. Chaque table a $\varphi(n)$ lignes et $\varphi(n)$ colonnes.

$n = 6$ $(2p)$

	1	5
1		5
5	5	

$n = 8$

	1	3	5	7
1		3	5	7
3	3		7	5
5	5	7		3
7	7	5	3	

$n = 10$ $(2p)$

	1	3	7	9
1		3	7	
3	3			7
7	7			3
9		7	3	

$n = 12$

	1	5	7	11
1		5	7	11
5	5		11	7
7	7	11		5
11	11	7	5	

$n = 14$ $(2p)$

	1	3	5	9	11	13
1		3	5		11	13
3	3			13	5	11
5	5		11	3	13	
9		13	3	11		5
11	11	5	13			3
13	13	11		5	3	

$n = 16$

	1	3	5	7	9	11	13	15
1		3	5	7		11	13	
3	3			5	11		7	13
5	5			3	13	7		11
7	7	5	3			13	11	
9		11	13			3	5	7
11	11		7	13	3			5
13	13	7		11	5			3
15		13	11		7	5	3	

$n = 18$

	1	5	7	11	13	17
1		5	7	11	13	17
5	5	7	17		11	13
7	7	17	13	5		11
11	11		5	13	17	7
13	13	11		17	7	5
17	17	13	11	7	5	

$n = 20$

	1	3	7	9	11	13	17	19
1		3	7		11	13	17	19
3	3			7	13	19	11	17
7	7			3	17	11	19	13
9		7	3		19	17	13	11
11	11	13	17	19		3	7	
13	13	19	11	17	3			7
17	17	11	19	13	7			3
19	19	17	13	11		7	3	

*. On ne peut s'empêcher de penser à un mirage, une chimère...

†. ceci pour tout $n \geq 300$ et $n < 10^6$ car en deçà de 300, il y a quelques exceptions, les nombres 8, 12, 44, 104, 128, 152, 170, 212, 248 et 296.

$n = 22$ $(2p)$

	1	3	5	7	9	13	15	17	19	21
1		3	5	7		13		17	19	
3	3				5	17		7	13	19
5	5		3	13				19	7	17
7	7		13	5	19	3	17			
9		5		19		7	3		17	13
13	13	17		3	7		19		5	
15				17	3	19	5	13		7
17	17	7	19				13	3		5
19	19	13	7		17	5				3
21		19	17		13		7	5	3	

$n = 24$

	1	5	7	11	13	17	19	23
1		5	7	11	13	17	19	23
5	5		11	7	17	13	23	19
7	7	11		5	19	23	13	17
11	11	7	5		23	19	17	13
13	13	17	19	23		5	7	11
17	17	13	23	19	5		11	7
19	19	23	13	17	7	11		5
23	23	19	17	13	11	7	5	

$n = 26$ $(2p)$

	1	3	5	7	9	11	15	17	19	21	23	25
1		3	5	7		11		17	19		23	
3	3					7	19		5	11	17	23
5	5				19	3	23	7	17		11	
7	7			23	11				3	17	5	19
9			19	11	3		5	23		7		17
11	11	7	3			17		5		23	19	
15		19	23		5		17			3	7	11
17	17		7		23	5		3	11	19		
19	19	5	17	3				11	23			7
21			11		17	7	23	3	19			5
23	23	17	11	5		19	7					3
25		23		19	17		11		7	5	3	

$n = 28$

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

$n = 30$

	1	7	11	13	17	19	23	29
1		7	11	13	17	19	23	29
7	7	19	17		29	13	11	23
11	11	17		23	7	29	13	19
13	13		23	19	11	7	29	17
17	17	29	7	11	19	23		13
19	19	13	29	7	23		17	11
23	23	11	13	29		17	19	7
29	29	23	19	17	13	11	7	

$n = 32$

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

$n = 34$ $(2p)$

	1	3	5	7	9	11	13	15	19	21	23	25	27	29	31	33
1		3	5	7		11	13		19		23			29	31	
3	3						5	11	23	29		7	13	19		31
5	5				11		31	7		3	13	23			19	29
7	7				29		23	3	31	11		5	19		13	
9			11	29	13	31				19	3		5	23	7	
11	11				31	19	7	29	5			3		13		23
13	13	5	31	23		7						19	11	3	29	
15		11	7	3		29			13		5		31		23	19
19	19	23		31		5		13			29		3	7	11	
21		29	3	11	19						7		23	31	5	13
23	23		13		3			5	29	7	19	31				11
25		7	23	5		3	19				31	13	29	11		
27		13		19	5		11	31	3	23		29				7
29	29	19			23	13	3		7	31		11				5
31	31		19	13	7		29	23	11	5						3
33		31	29			23		19		13	11		7	5	3	

$n = 36$

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

$n = 38$ $(2p)$

	1	3	5	7	9	11	13	15	17	21	23	25	27	29	31	33	35	37
1		3	5	7		11	13		17		23			29	31			37
3	3							7	13		31	37	5	11	17	23	29	
5	5				7	17		37		29		11		31	3	13	23	
7	7			11				29	5			23	37	13		3	17	31
9			7		5	23	3			37	17				13	31	11	29
11	11		17		23	7	29	13		3			31		37		5	
13	13				3	29	17	5	31	7					23	11	37	
15		7	37	29		13	5			11	3			17			31	23
17	17	13		5			31		23		11	7	3	37		29		
21			29		37	3	7	11		23		31			5		13	17
23	23	31			17			3	11			5	13		29	37	7	
25		37	11	23					7	31	5	17	29	3				13
27		5		37		31			3		13	29	7	23		17		11
29	29	11	31	13				17	37			3	23	5		7		
31	31	17	3		13	37	23			5	29				11			7
33		23	13	3	31		11		29		37		17	7				5
35		29	23	17	11	5	37	31		13	7							3
37	37			31	29			23		17		13	11		7	5	3	

$n = 40$

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

$n = 42$

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

$n = 44$

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

$n = 46\ \ (2p)$

	1	3	5	7	9	11	13	15	17	19	21	25	27	29	31	33	35	37	39	41	43	45
1		3	5	7		11	13		17	19				29	31			37		41	43	
3	3								5	11	17	29		41		7	13	19		31	37	43
5	5						19	29		3	13		43	7	17		37		11		31	41
7	7			3	17	31		13		41		37	5	19				29	43	11		
9				17		7		43			5	41	13	31	3			11	29		19	37
11	11			31	7	29	5		3					43	19	41	17			37	13	
13	13		19			5	31	11	37	17	43	3	29				41				7	
15			29	13	43		11	41				7	37		5		19	3		17		31
17	17	5				3	37		13			11					43	31	19	7	41	29
19	19	11	3	41			17				31		7		37	29		13	5	43		
21		17	13		5		43			31		19		11	7	3		41	37		29	
25		29		37	41		3	7	11		19		31			43		5		13	17	
27			43	5	13		29	37		7		31				17			41	3	11	19
29	29	41	7	19	31	43					11			13		37	3				5	17
31	31		17		3	19		5		37	7				41	11		43	13	29		
33		7				41				29	3	43	17	37	11	31	5			19		13
35		13	37			17	41	19	43					3		5	29	7	31			11
37	37	19		29	11			3	31	13	41	5			43		7		17			
39			11	43	29				19	5	37		41		13		31	17	3			7
41	41	31		11		37		17	7	43		13	3		29	19						5
43	43	37	31		19	13	7		41		29	17	11	5								3
45		43	41		37			31	29				19	17		13	11		7	5	3	

$n = 48$

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

$n = 50$

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

$n = 52$

	1	3	5	7	9	11	15	17	19	21	23	25	27	29	31	33	35	37	41	43	45	47	49	51
1		3	5	7		11		17	19		23			29	31			37	41	43		47		
3	3								5	11	17	23	29		41	47		7	19		31	37	43	
5	5					3	23		43		11		31	41			19	29		7	17		37	47
7	7				11				29	43	5	19		47		23	37			41	3	17	31	
9				11	29	47	31					17			19	37	3		5	23	41	7		43
11	11		3		47	17		31		23			37	7	29			43		5			19	41
15			23		31		17	47		3		11	41	19			5		43			29	7	37
17	17					31	47	29	11				43		7	41	23	5		3	37	19		
19	19	5	43	29				11				7		31	17	3	41			37	23		47	
21		11		43		23	3					5	47	37		17	7		29	19			41	31
23	23	17	11	5								3		43	37	31		19	7		47	41		29
25		23		19	17		11		7	5	3				47		43	41	37			31	29	
27		29	31			37	41	43		47				3	5	7		11		17	19		23	
29	29		41	47		7	19		31	37	43		3								5	11	17	23
31	31	41			19	29		7	17		37	47	5					3	23		43		11	
33		47		23	37			41	3	17	31		7				11				29	43	5	19
35			19	37	3		5	23	41	7		43				11	29	47	31					17
37	37	7	29			43		5			19	41	11		3		47	17		31		23		
41	41	19			5		43			29	7	37			23		31		17	47		3		11
43	43		7	41	23	5		3	37	19			17					31	47	29	11			
45		31	17	3	41			37	23		47		19	5	43	29				11				7
47	47	37		17	7		29	19			41	31		11		43		23	3					5
49		43	37	31		19	7		47	41		29	23	17	11	5								3
51			47		43	41	37			31	29			23		19	17		11		7	5	3	

$n = 54$

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

$n = 56$

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

$n = 58$ $(2p)$

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

$n = 60$

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

On dispose des connaissances éparses suivantes qui pourraient être utiles :

→ pour tous p, q, nombres premiers à n, on a $p^{(q-1)/2} \equiv \pm 1 \ (mod\ q)$ selon que p est (+1) ou n'est pas (-1) résidu quadratique de q ;
→ pour tout p premier à n, $p^{\varphi(n)} \equiv 1 \ (mod\ n)$;

→ si n est de la forme $4k+2$ (n double d'impair) alors pour $m \leq n/4$, $\left(\frac{x}{n}\right) = \left(\frac{x+m}{n}\right)$;

→ article 78 des Recherches arithmétiques : le produit des unités (des nombres premiers à n) est congru à -1 ($mod\ n$) pour n double d'une puissance de nombre premier différent de 2 (ainsi que pour $n = 4$ ou $n = p^m$) ; il est congru à 1 pour les autres nombres pairs ;

→ -1 est résidu quadratique des nombres premiers de la forme $4k+1$ ou bien des nombres composés de la forme $4k+1$ qui ne contiennent aucun premier $4k+3$ dans leur factorisation ;

→ -1 est non résidu quadratique des nombres pairs de la forme $4k$; il est résidu quadratique des nombres pairs de la forme $4k+2$ sauf s'ils contiennent un $4k+3$ dans leur factorisation et -1 est non-résidu quadratique de tous les autres nombres pairs qui ne contiennent aucun $4k+3$ dans leur factorisation.