Pgcd et diagonales de booléens (Denise Vella-Chemla, 22.10.2016)

Dans une note récente, on a calculé par programme les racines de l'unité (notées x) des entiers successifs (notés n), i.e. les nombres dont la division d'une puissance x^k par n avait pour reste 1 (x est tel que $\exists k, 1 \leqslant k \leqslant n-1,\ x^k \equiv 1\ (mod\ n)$). On rappelle que deux nombres *premiers entre eux* ont un plus grand commun diviseur ($pgcd(x,n)$) égal à 1. On a réalisé en étudiant les racines de l'unité que seul un nombre *premier à* n peut avoir l'une de ses puissances congrue à 1 modulo n.

On se propose ici d'étudier une table de booléens associés à la relation *premier à* qui lie deux nombres. Dans cette table, pour les nombres x compris entre 3 et 51, on note pour chaque nombre y compris entre 1 et $\left\lfloor \frac{x}{2} \right\rfloor$ la valeur de vérité (booléenne) de $(x,y) = 1$ (le booléen de la case (x,y) de la table vaut donc 1 pour tout nombre y premier à x et 0 pour les autres s'il y en a)[1]. On note en rouge les diagonales de 1 "issues" du nombre premier 23.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
3 :	1																								
4 :	1	0																							
5 :	1	1																							
6 :	1	0	0																						
7 :	1	1	1																						
8 :	1	0	1	0																					
9 :	1	1	0	1																					
10 :	1	0	1	0	0																				
11 :	1	1	1	1	1																				
12 :	1	0	0	0	1	0																			
13 :	1	1	1	1	1	1																			
14 :	1	0	1	0	1	0	0																		
15 :	1	1	0	1	0	0	1																		
16 :	1	0	1	0	1	0	1	0																	
17 :	1	1	1	1	1	1	1	1																	
18 :	1	0	0	0	1	0	1	0	0																
19 :	1	1	1	1	1	1	1	1	1																
20 :	1	0	1	0	0	0	1	0	1	0															
21 :	1	1	0	1	1	0	0	1	0	1															
22 :	1	0	1	0	1	0	1	0	1	0	0														
23 :	1	1	1	1	1	1	1	1	1	1	1														
24 :	1	0	0	0	1	0	1	0	0	0	1	0													
25 :	1	1	1	1	0	1	1	1	1	0	1	1													
26 :	1	0	1	0	1	0	1	0	1	0	1	0	0												
27 :	1	1	0	1	1	0	1	1	0	1	1	0	1												
28 :	1	0	1	0	1	0	0	0	1	0	1	0	1	0											
29 :	1	1	1	1	1	1	1	1	1	1	1	1	1	1											
30 :	1	0	0	0	0	0	1	0	0	0	1	0	1	0	0										
31 :	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1										
32 :	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0									
33 :	1	1	0	1	1	0	1	1	0	1	0	0	1	1	0	1									
34 :	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0								
35 :	1	1	1	1	0	1	0	1	1	0	1	1	1	0	0	1	1								
36 :	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0							
37 :	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1							
38 :	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0						
39 :	1	1	0	1	1	0	1	1	0	1	1	0	0	1	0	1	1	0	1						
40 :	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0					
41 :	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1					
42 :	1	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	1	0	1	0	0				
43 :	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1				
44 :	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0			
45 :	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0	1	1	0	1	0	0	1			
46 :	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0		
47 :	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
48 :	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	
49 :	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	
50 :	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0
51 :	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	0	0	1	1	0	1	1	0	1

Aux nombres premiers correspondent ainsi des diagonales de plus grands communs diviseurs valant 1 :

$$\forall\ p\ premier, \quad \begin{array}{l} \forall x, 1 \leqslant x \leqslant \lfloor \frac{p-1}{3} \rfloor, (p-x, x) = 1. \\ \forall x, 1 \leqslant x \leqslant p-1, (p+x, x) = 1. \end{array}$$

[1] On note parfois le plus grand commun diviseur de x et y ($pgcd(x,y)$) en utilisant le symbole $\wedge$ (et logique) : $x \wedge y = 1$).