Des puissances et des palindromes (Denise Vella-Chemla, 18.5.2019)

On présente ici une découverte de propriétés palindromiques des puissances des nombres dans les corps premiers.

On se place dans un corps premier $\mathbb{Z}/p\mathbb{Z}$ et on regroupe les nombres 4 par 4 : chaque quadruplet q_n contient un nombre n, son opposé $-n$, son inverse $1/n$ et l'opposé de son inverse $-1/n$. On considère également la fonction qui, inversement [1], associe aux nombres n, $-n$, $1/n$ et $-1/n$ l'indice q_n du quadruplet auquel ils appartiennent.

Pour avoir une image en tête, on peut visualiser les nombres de 1 à $p-1$ aux 4 coins de carrés qu'on aurait empilés comme les étages d'un immeuble et les q_n sont les numéros des étages.

Un nombre premier p a comme propriété que tout nombre de 1 à $p-1$ est égal à une puissance d'une racine primitive de p. En étudiant les puissances en question, ou plutôt leur étage associé, on va voir que les étages ne sont pas parcourus aléatoirement, mais selon un ordre doublement palindromique.

Expliquons ces idées sur un exemple. Ci-dessous, on fournit les (plus petites) racines primitives des nombres premiers de 11 à 100 qu'on a utilisées.

11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
7	7	3	3	7	3	3	19	7	3	11	3	11	7	7	7	11	3	19	3	7

Voici les différents quadruplets de nombres associés à 97 et les puissances de 7 prise comme racine primitive de 97 dans le corps premier $\mathbb{Z}/97\mathbb{Z}$.

$1 \mapsto (2, 49, 95, 48)$	$13 \mapsto (18, 27, 70, 79)$
$2 \mapsto (3, 32, 65, 94)$	$14 \mapsto (19, 46, 51, 78)$
$3 \mapsto (4, 24, 73, 93)$	$15 \mapsto (20, 34, 63, 77)$
$4 \mapsto (5, 39, 58, 92)$	$16 \mapsto (21, 37, 60, 76)$
$5 \mapsto (6, 16, 81, 91)$	$17 \mapsto (22, 0, 0, 75)$
$6 \mapsto (7, 14, 83, 90)$	$18 \mapsto (23, 38, 59, 74)$
$7 \mapsto (8, 12, 85, 89)$	$19 \mapsto (25, 31, 66, 72)$
$8 \mapsto (9, 43, 54, 88)$	$20 \mapsto (26, 41, 56, 71)$
$9 \mapsto (10, 29, 68, 87)$	$21 \mapsto (28, 45, 52, 69)$
$10 \mapsto (11, 44, 53, 86)$	$22 \mapsto (30, 42, 55, 67)$
$11 \mapsto (13, 15, 82, 84)$	$23 \mapsto (33, 47, 50, 64)$
$12 \mapsto (17, 40, 57, 80)$	$24 \mapsto (35, 36, 61, 62)$

$7^{1} = 7$	$7^{21} = 63$	$7^{41} = 82$	$7^{61} = 59$	$7^{81} = 46$
$7^{2} = 49$	$7^{22} = 53$	$7^{42} = 89$	$7^{62} = 25$	$7^{82} = 31$
$7^{3} = 52$	$7^{23} = 80$	$7^{43} = 41$	$7^{63} = 78$	$7^{83} = 23$
$7^{4} = 73$	$7^{24} = 75$	$7^{44} = 93$	$7^{64} = 61$	$7^{84} = 64$
$7^{5} = 26$	$7^{25} = 40$	$7^{45} = 69$	$7^{65} = 39$	$7^{85} = 60$
$7^{6} = 85$	$7^{26} = 86$	$7^{46} = 95$	$7^{66} = 79$	$7^{86} = 32$
$7^{7} = 13$	$7^{27} = 20$	$7^{47} = 83$	$7^{67} = 68$	$7^{87} = 30$
$7^{8} = 91$	$7^{28} = 43$	$7^{48} = 96$	$7^{68} = 88$	$7^{88} = 16$
$7^{9} = 55$	$7^{29} = 10$	$7^{49} = 90$	$7^{69} = 34$	$7^{89} = 15$
$7^{10} = 94$	$7^{30} = 70$	$7^{50} = 48$	$7^{70} = 44$	$7^{90} = 8$
$7^{11} = 76$	$7^{31} = 5$	$7^{51} = 45$	$7^{71} = 17$	$7^{91} = 56$
$7^{12} = 47$	$7^{32} = 35$	$7^{52} = 24$	$7^{72} = 22$	$7^{92} = 4$
$7^{13} = 38$	$7^{33} = 51$	$7^{53} = 71$	$7^{73} = 57$	$7^{93} = 28$
$7^{14} = 72$	$7^{34} = 66$	$7^{54} = 12$	$7^{74} = 11$	$7^{94} = 2$
$7^{15} = 19$	$7^{35} = 74$	$7^{55} = 84$	$7^{75} = 77$	$7^{95} = 14$
$7^{16} = 36$	$7^{36} = 33$	$7^{56} = 6$	$7^{76} = 54$	$7^{96} = 1$
$7^{17} = 58$	$7^{37} = 37$	$7^{57} = 42$	$7^{77} = 87$	
$7^{18} = 18$	$7^{38} = 65$	$7^{58} = 3$	$7^{78} = 27$	
$7^{19} = 29$	$7^{39} = 67$	$7^{59} = 21$	$7^{79} = 92$	
$7^{20} = 9$	$7^{40} = 81$	$7^{60} = 50$	$7^{80} = 62$	

1. au sens fonctionnel cette fois.

Si maintenant on écrit, dans l'ordre des puissances successives ci-dessus, les indices des quadruplets correspondant, on obtient l'ordre suivant de parcours des "étages" de l'immeuble des petits carrés (ou quadruplets) :

$7^{1} \to 6$	$7^{25} \to 12$	$7^{49} \to 6$	$7^{73} \to 12$
$7^{2} \to 1$	$7^{26} \to 10$	$7^{50} \to 1$	$7^{74} \to 10$
$7^{3} \to 21$	$7^{27} \to 15$	$7^{51} \to 21$	$7^{75} \to 15$
$7^{4} \to 3$	$7^{28} \to 8$	$7^{52} \to 3$	$7^{76} \to 8$
$7^{5} \to 20$	$7^{29} \to 9$	$7^{53} \to 20$	$7^{77} \to 9$
$7^{6} \to 7$	$7^{30} \to 13$	$7^{54} \to 7$	$7^{78} \to 13$
$7^{7} \to 11$	$7^{31} \to 4$	$7^{55} \to 11$	$7^{79} \to 4$
$7^{8} \to 5$	$7^{32} \to 24$	$7^{56} \to 5$	$7^{80} \to 24$
$7^{9} \to 22$	$7^{33} \to 14$	$7^{57} \to 22$	$7^{81} \to 14$
$7^{10} \to 2$	$7^{34} \to 19$	$7^{58} \to 2$	$7^{82} \to 19$
$7^{11} \to 16$	$7^{35} \to 18$	$7^{59} \to 16$	$7^{83} \to 18$
$7^{12} \to 23$	$7^{36} \to 23$	$7^{60} \to 23$	$7^{84} \to 23$
$7^{13} \to 18$	$7^{37} \to 16$	$7^{61} \to 18$	$7^{85} \to 16$
$7^{14} \to 19$	$7^{38} \to 2$	$7^{62} \to 19$	$7^{86} \to 2$
$7^{15} \to 14$	$7^{39} \to 22$	$7^{63} \to 14$	$7^{87} \to 22$
$7^{16} \to 24$	$7^{40} \to 5$	$7^{64} \to 24$	$7^{88} \to 5$
$7^{17} \to 4$	$7^{41} \to 11$	$7^{65} \to 4$	$7^{89} \to 11$
$7^{18} \to 13$	$7^{42} \to 7$	$7^{66} \to 13$	$7^{90} \to 7$
$7^{19} \to 9$	$7^{43} \to 20$	$7^{67} \to 9$	$7^{91} \to 20$
$7^{20} \to 8$	$7^{44} \to 3$	$7^{68} \to 8$	$7^{92} \to 3$
$7^{21} \to 15$	$7^{45} \to 21$	$7^{69} \to 15$	$7^{93} \to 21$
$7^{22} \to 10$	$7^{46} \to 1$	$7^{70} \to 10$	$7^{94} \to 1$
$7^{23} \to 12$	$7^{47} \to 6$	$7^{71} \to 12$	$7^{95} \to 6$
$7^{24} \to 17$	$7^{48} \to -$	$7^{72} \to 17$	

On repère bien l'identité des images entre la première et la troisième colonne ou bien entre la seconde et la quatrième colonne ainsi que l'ordre inversé des nombres de la première à la seconde colonne par exemple. Ces propriétés de palindromie des images s'observent pour tous les nombres premiers inférieurs à 100 et doivent donc être démontrable. La palindromie ayant lieu à la fois sur la séquence totale de quadruplets ainsi que sur chacune des moitiés de la séquence prises séparément, on a du coup une périodicité sur la séquence globale, de longueur la moitié de la longueur totale. Cette longueur vaut $p - 1$ pour les nombres premiers, elle est moindre pour les nombres composés.

Concernant maintenant les modules composés, du fait que certains nombres inférieurs à eux partagent avec eux certains diviseurs, on perd cette possibilité qu'une racine primitive permette d'obtenir tous les nombres du corps premier par élévation à toutes les puissances. Outre ce fait que certains indices de groupes ne puissent jamais être atteints par les puissances, on constate parfois de minuscules "défauts de palindromie", notamment pour des puissances de nombres premiers, dont on donne simplement quelques exemples ci-dessous.

En prenant comme racine primitive 3 pour le module 25, on obtient les puissances et les indices du tableau ci-dessous. 19 nombres sont atteints. Le centre du mot palindrome est coloré en bleu, le défaut de palindromie en rouge.

3	9	2	6	18	4	12	11	8	24	22	16	23	19	7	21	13	14	17
2	6	1	3	5	3	1	6	2	1	2	6	8	3	5	3	1	6	2

En prenant comme racine primitive 5 pour le module 27, on obtient les puissances et les indices du tableau ci-dessous. Les palindromies, à gauche du milieu, à droite, ainsi que globale, sont toutes respectées ; du coup, il y a périodicité puisque moitié gauche et droite de la séquence sont égales. Cependant, seulement 17 quadruplets sont atteints (17 n'est pas égal à $27 - 1$).

5	25	17	4	20	19	14	16	26	22	2	10	23	7	8	13	11
4	1	6	3	3	6	1	4	1	4	1	6	3	3	6	1	4

En prenant comme racine primitive 3 ou 11 pour le module 49, les palindromies sont respectées mais ce n'est pas le cas pour la racine primitive 5 pour laquelle on a :

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

On essaie deux exemples de modules supplémentaires, qui sont deux puissances de nombres premiers : $81 = 3^4$ et $121 = 11^2$.

Pour 81 avec 5 comme racine primitive, 5^{20} est dans le quadruplet (étage) 27 quand 5^{34} est dans le quadruplet 1, la palindromie globale n'est pas respectée à une puissance près. Pour 121 de racine primitive 7, c'est 7^8 qui se retrouve dans le quadruplet 33 quand 7^{55} est dans le quadruplet 1.