Tables de résidus quadratiques des modules 3 à 51 (Denise Vella-Chemla, 16.8.16)

Voici les tables qui permettent d'induire, de visu, mais cela ne reste qu'une hypothèse :

- que les nombres premiers de la forme $4k+3$ ont strictement plus de $n/4$ résidus quadratiques inférieurs ou égaux à leur moitié ;
- que les nombres premiers de la forme $4k+1$ ont $(n-1)/4$ résidus quadratiques inférieurs ou égaux à leur moitié ;
- que les nombres composés ont moins de $n/4$ résidus quadratiques inférieurs ou égaux à leur moitié.

On commence par calculer les carrés modulo le nombre n considéré et les noter dans la troisième ligne, sous la barre. Puis on colorie leur occurrence dans les deux premières lignes. Enfin, on compte les petits résidus quadratiques (notés *prq*, i.e. ceux qui sont inférieurs à $n/2$, et qui apparaissent dans la seconde ligne).

Module $n = 3$ (1 prq $> 3/4$)

2
1
1

Module $n = 5$ (1 prq)

4	3
1	2
1	4

Module $n = 7$ (2 prq $> 7/4$)

6	5	4
1	2	3
1	4	2

Module $n = 9$ (2 prq $< 9/4$)

8	7	6	5
1	2	3	4
1	4	0	7

Module $n = 11$ (4 prq $> 11/4$)

10	9	8	7	6
1	2	3	4	5
1	4	9	5	3

Module $n = 13$ (3 prq $= 13/4$)

12	11	10	9	8	7
1	2	3	4	5	6
1	4	9	3	12	10

Module $n = 15$ (3 prq $< 15/4$)

14	13	12	11	10	9	8
1	2	3	4	5	6	7
14	9	1	10	6	4	

Module $n = 17$ (4 prq $= 17/4$)

16	15	14	13	12	11	10	9
1	2	3	4	5	6	7	8
1	4	9	16	8	2	15	13

Module $n = 19$ (6 prq $> 19/4$)

18	17	16	15	14	13	12	11	10
1	2	3	4	5	6	7	8	9
1	4	9	16	6	17	11	7	5

Module $n = 21$ (4 prq $< 21/4$)

20	19	18	17	16	15	14	13	12	11
1	2	3	4	5	6	7	8	9	10
1	4	9	16	4	15	7	1	18	16

Module $n = 23$ (7 prq $> 23/4$)

22	21	20	19	18	17	16	15	14	13	12
1	2	3	4	5	6	7	8	9	10	11
1	4	9	16	2	13	3	18	12	8	6

Module $n = 25$ (5 prq $< 25/4$)

24	23	22	21	20	19	18	17	16	15	14	13
1	2	3	4	5	6	7	8	9	10	11	12
1	4	9	16	0	11	24	14	6	0	21	19

Module $n = 27$ (6 prq $< 27/4$)

26	25	24	23	22	21	20	19	18	17	16	15	14
1	2	3	4	5	6	7	8	9	10	11	12	13
1	4	9	16	25	9	22	10	0	19	13	9	7

Module $n = 29$ (7 prq $> 29/4$)

28	27	26	25	24	23	22	21	20	19	18	17	16	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	4	9	16	25	7	20	6	23	13	5	28	24	22

Module $n = 31$ (9 prq $> 31/4$)

30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	4	9	16	25	5	18	2	19	7	28	20	14	10	8

Module $n = 33$ (7 prq $< 33/4$)

32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	4	9	16	25	3	16	31	15	1	22	12	4	31	27	25

Module $n = 35$ (7 prq $< 35/4$)

34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	4	9	16	25	1	14	29	11	30	16	4	29	21	15	11	9

Module $n = 37$ (9 prq $> 37/4$)

36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	4	9	16	25	36	12	27	7	26	10	33	21	11	3	34	30	28

Module $n = 39$ (8 prq $< 39/4$)

38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	4	9	16	25	36	10	25	3	22	4	27	13	1	30	22	16	12	10

Module $n = 41$ (10 prq $> 41/4$)

40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	4	9	16	25	36	8	23	40	18	39	21	5	32	20	10	2	37	33	31

Module $n = 43$ (12 prq $> 43/4$)

42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	4	9	16	25	36	6	21	38	14	35	15	40	24	10	41	31	23	17	13	11

Module $n = 45$ (6 prq $< 45/4$)

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

Module $n = 47$ (14 prq $> 47/4$)

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

Module $n = 49$ (11 prq $< 49/4$)

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

Module $n = 51$ (10 prq $< 51/4$)

50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26
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
1	4	9	16	25	36	49	13	30	49	19	42	16	43	21	1	34	18	4	43	33	25	19	15	13

On remarque enfin un élément qu'il est peut-être intéressant de souligner : selon le module $p = 23$ par exemple, les carrés s'obtenant par additions d'impairs successifs à partir de 0, on a la succession de restes modulaires suivante :

$$0 \xrightarrow{+1} 1 \xrightarrow{+3} 4 \xrightarrow{+5} 9 \xrightarrow{+7} 16 \xrightarrow{+9} 2$$

$$\xrightarrow{+11} 13 \xrightarrow{+13} 3 \xrightarrow{+15} 18 \xrightarrow{+17} 12 \xrightarrow{+19} 8 \xrightarrow{+21} 6$$

dans laquelle on compte 7 restes quadratiques inférieurs ou égaux à $11 = \dfrac{23-1}{2}$.

On obtient le même nombre de restes inférieurs ou égaux à $\frac{p-1}{2}$ dans la suite précédente que dans la suite obtenue en ajoutant des *pairs* successifs plutôt que des *impairs*, dans une suite commençant à $6 = \frac{p+1}{4}$.

$$6 \xrightarrow{+\,2} 8 \xrightarrow{+\,4} 12 \xrightarrow{+\,6} 18 \xrightarrow{+\,8} 3 \xrightarrow{+\,10} 13$$

$$\xrightarrow{+\,12} 2 \xrightarrow{+\,14} 16 \xrightarrow{+\,16} 9 \xrightarrow{+\,18} 4 \xrightarrow{+\,20} 1 \xrightarrow{+\,22} 0$$