Pile la moitié *(Denise Vella-Chemla, 17.10.2017)*

On rappelle la section 96 des Recherches arithmétiques de Gauss :

> *96. Le nombre premier p étant pris pour module, la moitié des nombres $1, 2, 3 \ldots p-1$, sera composée de résidus quadratiques, et l'autre moitié de non-résidus, c'est-à-dire qu'il y aura $\frac{1}{2}(p-1)$ résidus et autant de non-résidus.*
>
> *On prouve facilement que tous les carrés $1, 4, 9 \ldots \left(\frac{p-1}{2}\right)^2$ sont incongrus ; car si l'on pouvait avoir $r^2 \equiv r'^2 \pmod{p}$ et que les nombres r et r' fussent inégaux et $< \frac{p-1}{2}$, soit $r > r'$, on aurait $(r-r')(r+r')$, divisible par p ; mais chaque facteur étant $< p$, la proposition ne peut subsister. Il y a donc $\frac{p-1}{2}$ résidus quadratiques entre les nombres $1, 2, 3 \ldots p-1$; il ne peut y en avoir davantage, car en y joignant 0, le nombre en devient $\frac{1}{2}(p+1)$, limite qu'il ne peut pas dépasser. Donc les autres nombres seront non-résidus, et il y en aura $\frac{p-1}{2}$.*
>
> *Comme 0 est toujours résidu, nous l'excluons.*

Les nombres premiers p sont *les seuls* nombres à partager exactement l'ensemble des nombres compris entre 1 et $p-1$ en deux ensembles de même cardinal : l'ensemble des résidus quadratiques et l'ensemble des non-résidus quadratiques.

On illustre ci-dessous ce partage équitable des $p-1$ premiers entiers strictement positifs entre les résidus quadratiques et les non-résidus quadratiques modulo 17 (de la forme $4k+1$) et modulo 19 (de la forme $4k+3$). Les résidus quadratiques sont colorés en bleu. On a noté les valeurs des carrés pour rappel en bas, en deça du trait séparateur. L'usage de la couleur permet aussi de mettre en évidence, pour p premier, une relation entre le caractère de résiduosité quadratique d'un nombre x et celui de son complémentaire à p (ou $p - x = -x = (-1) \times x$).

Résidus quadratiques pour $p = 17$

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

Résidus quadratiques pour $p = 19$

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

On voit que pour p premier de la forme $4k+1$, x et $p-x$, dans la même colonne, sont soit tous deux résidus quadratiques, soit tous deux non-résidus quadratiques (cela est dû aux faits que $p - x = -x$ et que $p - 1 = -1$ est résidu quadratique).

Tandis que pour p de la forme $4k+3$, x est résidu quadratique équivaut à $p-x$ n'est pas résidu quadratique et inversement ($p - 1 = -1$ est alors non-résidu quadratique).

Ces équivalences ne sont pas vérifiées pour les nombres composés.

Pour le module 15, on a le petit tableau de Gauss des résidus quadratiques suivant :

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

Tout résidu quadratique r de tout nombre premier p vérifie la congruence :

$$r^{\frac{p-1}{2}} \equiv +1 \ (mod\ p)$$

tandis que tout non-résidu quadratique n de tout nombre premier p vérifie la congruence :

$$n^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$$

On vérifie ces congruences en calculant les valeurs des puissances $8^{èmes}$ des nombres modulo 17 ($8 = \frac{17-1}{2}$) et $9^{èmes}$ des nombres modulo 19 ($9 = \frac{18-1}{2}$) :

puissance	*valeur*	*classe* (*mod* 17)	*puissance*	*valeur*	*classe* (*mod* 19)
1^8	1	+1	1^9	1	+1
2^8	256	+1	2^9	512	−1
3^8	6 561	−1	3^9	19 683	−1
4^8	65 536	+1	4^9	262 144	+1
5^8	390 625	−1	5^9	1 953 125	+1
6^8	1 679 616	−1	6^9	10 077 696	+1
7^8	5 764 801	−1	7^9	40 353 607	+1
8^8	16 777 216	+1	8^9	134 217 728	−1
9^8	43 046 721	+1	9^9	387 420 480	+1
10^8	100 000 000	−1	10^9	1 000 000 000	−1
11^8	214 358 881	−1	11^9	2 357 947 691	+1
12^8	429 981 696	−1	12^9	5 159 780 352	−1
13^8	815 730 721	+1	13^9	10 604 499 373	−1
14^8	1 475 789 056	−1	14^9	20 661 046 784	−1
15^8	2 562 890 625	+1	15^9	38 443 359 375	−1
16^8	4 294 967 296	+1	16^9	68 719 476 736	+1
			17^9	118 587 876 497	+1
			18^9	198 359 290 368	−1

En annexe sont fournies les tables des résidus des puissances des nombres modulo 17 et 19.

Etudions maintenant les puissances successives modulaires de nombres (dont la racine carrée de la $(p-1)^{ème}$ puissance ou $\frac{1}{2}(p-1)^{ème}$ puissance). On peut voir la suite des puissances successives d'un résidu quadratique comme une suite (une chaîne orientée) $\mathcal{C}$ de $\frac{p-1}{2}$ nombres. Par l'opération d'inversion ($f : x \mapsto \frac{1}{x}$), on obtient une chaîne de nombres $\mathcal{C}'$ orientée dans l'ordre inverse de l'ordre des nombres dans $\mathcal{C}$.

Ci-dessous, les chaînes des 2^x et 9^x, tous résidus quadratiques modulo 17, en sens inverse l'une de l'autre, dont les nombres sont inverses 2 à 2 les uns des autres (par colonne).

x	1	2	3	4	5	6	7	8
2^x	2	$\to 4$	$\to 8$	$\to 16$	$\to 15$	$\to 13$	$\to 9$	$\to 1$
9^x	9	$\to 13$	$\to 15$	$\to 16$	$\to 8$	$\to 4$	$\to 2$	$\to 1$

Toute puissance d'un résidu quadratique est un résidu quadratique. Dans chaque colonne, les nombres sont inverses l'un de l'autre, par exemple, 15 et 8 sont inverses ($15 = \frac{1}{8}$) puisque $15 \times 8 = 120 \equiv 1 \ (mod\ 17)$ (*rappel: car* $119 = 7 \times 17$). De même, $2 = \frac{1}{9}$, $4 = \frac{1}{13}$,...

Voyons maintenant les chaînes des 3^x et 6^x, tous les deux non-résidus quadratiques modulo 17, les nombres des deux chaînes sont inverses 2 à 2 les uns des autres (par colonne), de même que dans le tableau précédent. On a indiqué les résidus par un R et les non-résidus par un N entre parenthèses.

x	1	2	3	4	5	6	7	8
3^x	3 (N)	$\to 9$ (R)	$\to 10$ (N)	$\to 13$ (R)	$\to 5$ (N)	$\to 15$ (R)	$\to 11$ (N)	$\to 16$ (R) ($\equiv -1$)
6^x	6 (N)	$\to 2$ (R)	$\to 12$ (N)	$\to 4$ (R)	$\to 7$ (N)	$\to 8$ (R)	$\to 14$ (N)	$\to 16$ (R) ($\equiv -1$)

Toute puissance paire d'un non-résidu quadratique est un résidu quadratique alors que toute puissance impaire d'un non-résidu quadratique est un résidu quadratique (selon l'adage "moins par moins donne plus"). On peut regarder les deux chaînes de nombres ci-dessus comme "faisant la navette" entre l'ensemble des résidus quadratiques et l'ensemble des non-résidus quadratiques. L'ensemble des résidus quadratiques forme un groupe pour la multiplication (on n'en sort pas en multipliant deux éléments) alors que l'ensemble des non-résidus quadratiques n'est pas un groupe puisque le résultat de la multiplication de deux non-résidus quadratiques est un résidu quadratique.

Voici les chaînes pour le module 19, on les a fait démarrer à 4 et 5 pour les résidus et à 2 et 10 pour les non-résidus :

x	1	2	3	4	5	6	7	8	9
4^x	4	$\to 16$	$\to 7$	$\to 9$	$\to 17$	$\to 11$	$\to 6$	$\to 5$	$\to 1$
5^x	5	$\to 6$	$\to 11$	$\to 17$	$\to 9$	$\to 7$	$\to 16$	$\to 4$	$\to 1$

x	1	2	3	4	5	6	7	8	9
2^x	2 (N)	$\to 4$ (R)	$\to 8$ (N)	$\to 16$ (R)	$\to 13$ (N)	$\to 7$ (R)	$\to 14$ (N)	$\to 9$ (R)	$\to 18$ (N) $(\equiv -1)$
10^x	10 (N)	$\to 5$ (R)	$\to 12$ (N)	$\to 6$ (R)	$\to 3$ (N)	$\to 11$ (R)	$\to 15$ (N)	$\to 17$ (R)	$\to 18$ (N) $(\equiv -1)$

Seuls les nombres premiers ont pour propriété de partager l'ensemble des résidus quadratiques exactement en 2. Du fait de redondances intervenant dans les factorisations ($4 \times 6 = 3 \times 8$ par exemple), les nombres composés ont moins de résidus quadratiques que de non-résidus quadratiques.

En s'aidant du tableau des résidus des puissances modulaires pour le module $x = 15$ fourni en annexe, on constate qu'aucune puissance $\frac{1}{2}(x-1)^{ème}$ n'est égale à 1, seule la puissance $\frac{1}{2}(x-1)^{ème}$ de $x - 1 = 14$ est égal à $-1 = 14$ et seules les puissances $(x-1)^{èmes}$ des nombres 4, 11 et 14 sont égales à 1 alors qu'on a vu que 4 est résidu quadratique de 15 quand 11 et 14 ne le sont pas. Pour les nombres composés, on ne peut établir de caractéristique générale, comme on a pu le faire pour les nombres premiers.

Résumons ce qui a été présenté.

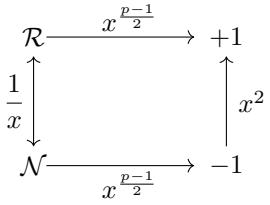
Pour p premier, si on note $\mathcal{R} = \{x / x^{\frac{p-1}{2}} \equiv +1 \ (mod\ p)\}$ et $\mathcal{N} = \{x / x^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)\}$, on a les chaînes d'élévations successives au carré suivantes, dans le groupe des résidus quadratiques :

$$f \quad : \underset{R}{x_1} \mapsto \underset{R}{x_2} \mapsto \underset{R}{x_3} \ldots \mapsto \mathbf{1} = \underset{R}{x_1}^{\frac{p-1}{2}}$$

et alternativement de l'ensemble des non-résidus quadratiques vers l'ensemble des résidus quadratiques :

$$g \quad : \underset{N}{y_1} \mapsto \underset{R}{y_2} \mapsto \underset{N}{y_3} \mapsto \underset{R}{y_4} \ldots \mapsto \mathbf{\text{-}1} = \underset{N}{y_1}^{\frac{p-1}{2}}$$

Un schéma résume la constitution des chaînes.



Lorsqu'on développe la fonction zêta de Riemann, on obtient :

$$\zeta(a+ib) = 1 + \left(\frac{1}{2}\right)^a e^{-ib\ ln\ 2} + \left(\frac{1}{3}\right)^a e^{-ib\ ln\ 3} + \left(\frac{1}{4}\right)^a e^{-ib\ ln\ 4} + \ldots$$

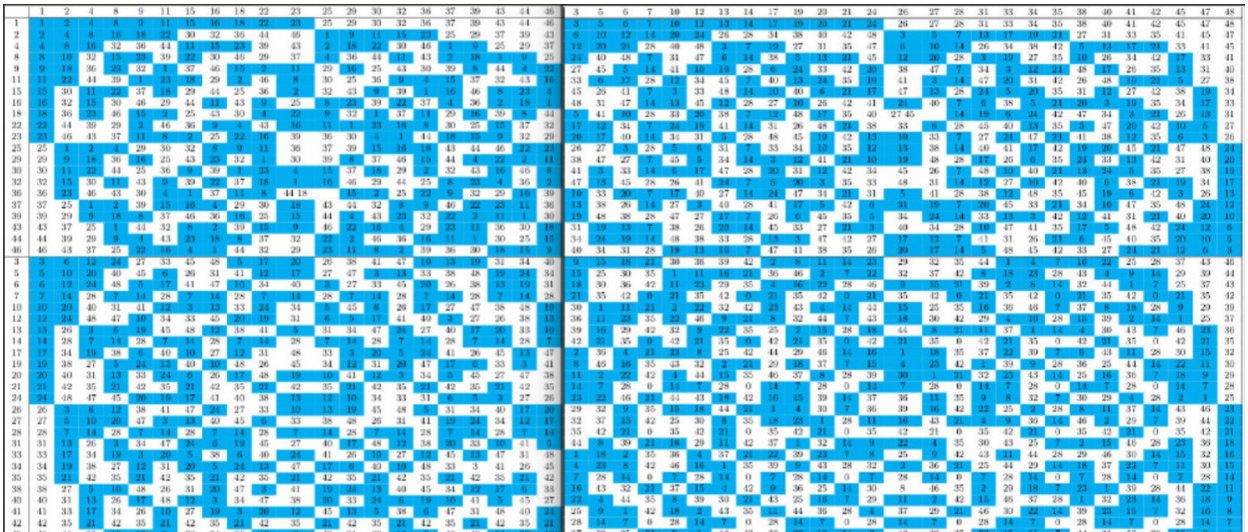
Quand $a = \frac{1}{2}$, pour les points du plan complexe situés sur la droite critique (points de partie réelle égale à $\frac{1}{2}$), les fractions devant chaque exponentielle sont les inverses des racines carrés des nombres entiers successifs : $\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{4}}, \ldots$.

Un nombre premier (appelons le p) symétrise l'espace constitué de l'ensemble des nombres en établissant des relations particulières et systématiques entre un nombre x et son complémentaire à p $(p-x)$. On avait déjà présenté cette symétrie que l'on voit aisément dans les tables de multiplication suivantes, la première étant la table du nombre premier 23 et la seconde étant celle du nombre composé 49.

La table de multiplication de 23 qui présente symétrise les résidus qudratiques et les non-résidus quadratiques :

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

La table de multiplication de 49 qui ne symétrise pas les résidus qudratiques et les non-résidus quadratiques



De manière anecdotique, les éléments caractéristiques qui ont été identifiés permettraient de représenter un nombre premier p par $1+log_2\left(\frac{p-1}{2}\right)$ booléens, correspondant aux caractères de résiduosité quadratique des nombres de 1 à $\frac{p-1}{2}$ que l'on fait précéder d'un booléen qui exprime que le nombre p est de la forme $4k+1$ ou $4k+3$ (on code -1 par 0).

La loi de réciprocité quadratique facilite le calcul des relations qui lie deux nombres ($(x\ R\ y)$ *ou* $(x\ N\ y)$ d'une part et ($(y\ R\ x)$ *ou* $(y\ N\ x)$) d'autre part) : on a une relation symétrique $(x\ R\ y)$ *et* $(y\ R\ x)$ dès que l'un des 2 nombres est de la forme $4k+1$, on a une relation anti-symétrique

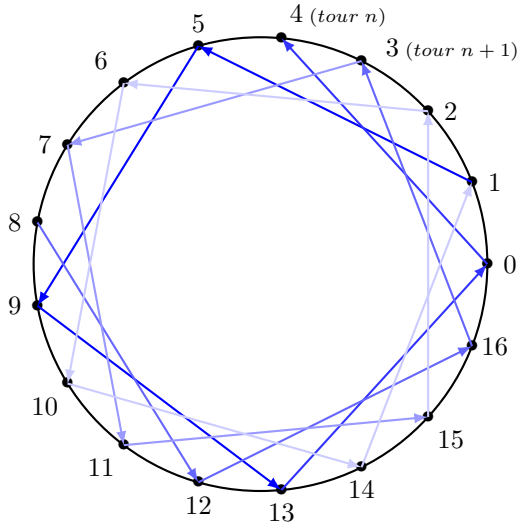
$$((x\ R\ y)\ et\ (y\ N\ x))\ ou\ exclusif\ ((xNy)\ et\ (y\ N\ x))$$

si les deux sont de la forme $4k+3$.

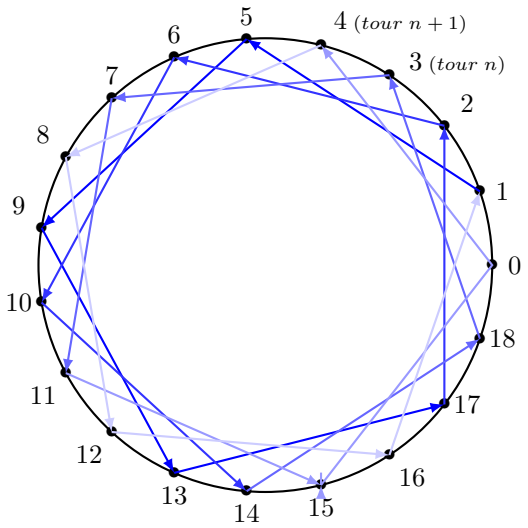
La notion d'orientation de chaînes de nombres fait toucher du doigt cette grande complexité de la loi de réciprocité quadratique : si l'on place les classes de restes sur un cercle et qu'on relie entre eux des

nombres espacés de 4, on voit que d'un tour à l'autre, les restes augmentent pour le module 17 de la forme $4k+1$ tandis qu'ils diminuent pour le module 19 de la forme $4k+3(=4k-1)$ (on indique cela en notant symboliquement les indices de deux tours successifs n et $n+1$ pour les restes 3 et 4 (pris au hasard) sur chaque cercle, en dégradant davantage le bleu à chaque tour - on voit que le dégradé décroît dans le sens anti-horaire pour le module 17 et dans le sens horaire pour 19, et en orientant les liens (correspondant à l'opération +4) par des flèches).

Cycle des restes des $4k+1$ *ou des* $4k+3$ *successifs modulo* $p=17$



Cycle des restes des $4k+1$ *ou des* $4k+3$ *successifs modulo* $p=19$



Rappelons d'une autre manière ce qui a été vu (et qui est connu depuis Gauss) : un nombre p est premier s'il partage l'ensemble des nombres de 1 à $p-1$ en deux ensembles que l'on peut mettre en bijection car ils sont de même cardinal. Ces deux ensembles sont l'ensemble des résidus quadratiques de p et l'ensemble des non-résidus quadratiques de p. Il y a exactement $\frac{p-1}{2}$ résidus et le même nombre de non-résidus lorsque p est premier.

Les résidus sont les $\frac{p-1}{2}$ solutions (notées par la variable x) de l'équation :

$$x^{\frac{p-1}{2}} - py - 1 = 0$$

avec x entier compris au sens large entre 1 et $p-1$, et y entier positif.

Les non-résidus sont les $\frac{p-1}{2}$ solutions de l'équation :

$$x^{\frac{p-1}{2}} - py + 1 = 0$$

dans les mêmes conditions.

On peut imaginer l'espace des nombres comme un polyèdre composé de multiples petites faces triangulaires, chacune autour d'un nombre et une petite boule à deux hémisphères, l'un noir (pour 1), l'autre blanc (pour -1), sur lesquels une fonction envoie les faces. Les faces correspondant aux nombres résidus quadratiques ont pour image 1, i.e. "s'envoient" sur l'hémisphère noir, tandis que celles qui correspondent aux non-résidus quadratiques s'envoient sur l'hémisphère blanc.

Prenons un exemple : les résidus quadratiques de 11 sont les entiers x compris entre 1 et 10 tels qu'il existe un y entier positif avec $x^5 - 11y - 1 = 0$. On a

$$\begin{aligned}
1^5 - 11 \times 0 - 1 &= 0 \\
3^5 - 11 \times 22 - 1 &= 0 \\
4^5 - 11 \times 93 - 1 &= 0 \\
5^5 - 11 \times 284 - 1 &= 0 \\
9^5 - 11 \times 5368 - 1 &= 0
\end{aligned}$$

donc 1, 3, 4, 5 et 9 sont résidus quadratiques de 11.

Les non-résidus quadratiques de 11 sont les entiers x compris entre 1 et 10 tels qu'il existe un y entier positif avec $\mathrm{x}^5 - 11y + 1 = 0$.

On a

$$\begin{aligned}
2^5 - 11 \times 3 + 1 &= 0 \\
6^5 - 11 \times 707 + 1 &= 0 \\
7^5 - 11 \times 1528 + 1 &= 0 \\
8^5 - 11 \times 2979 + 1 &= 0 \\
10^5 - 11 \times 9091 + 1 &= 0
\end{aligned}$$

donc 2, 6, 7, 8 et 10 sont non-résidus quadratiques de 11.

Aux nombres premiers de la forme $4k + 1$ (milieu pair, symétrie exacte des couleurs) correspondent des variétés de degré de plus en plus grand mais pair tandis qu'aux nombres premiers de la forme $4k + 3$ (milieu impair, nombres en bijection de couleurs inverse l'une de l'autre) correspondent des variétés de degré de plus en plus grand mais impair.

Sur les variétés correspondant aux nombres composés, il n'y a pas de symétrie ou anti-symétrie systématique entre les images par la fonction $x^{\frac{p-1}{2}}$ (qui vaut 1 ou -1) des points entiers résidu quadratique et non-résidu quadratique qui sont en bijection.

Annexe : Tables des résidus modulaires des puissances des nombres modulo 17, 19 et 15

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

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

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