Les rayons des permutations spirales

Jean-Guillaume Dumas

Les rayons des permutations spirales

Jean-Guillaume Dumas *

Résumé

Nous donnons une nouvelle caractérisation des quenines, puis prouvons la conjecture de [Dumas, 2008] sur l'orientation des rayons spirales. Nous donnons les équivalences entre les permutations définies par [Asveld, 2009] et les quenines, pérecquines, mongines de Jacques Roubaud, ainsi que la que la quatrième variante possible, ici dénommée roubine. Ensuite, nous démontrons la conjecture [Asveld, 2009, Conjecture 7.2], qui relie les permutations spirales aux générateurs congruentiels linéaires. Enfin nous en déduisons une définition générale de permutation spirale pour tout entier.

Mots-clefs : Permutation de Queneau-Daniel ; Quenine ; Rayon de spirale ; Roubine ; Sextine ; Spirale ; Spinine.

1 Introduction

Nous considérons la permutation δ_n définie comme suit [Audin, 2007] :

$$\delta_n(x) = \begin{cases} 2x & \text{si } 2x \leq n \\ 2n+1-2x & \text{sinon} \end{cases}$$

L'idée est de considérer les entiers modulo $2n+1$. Dans ce cas, $\delta_n(x)$ est simplement plus ou moins $2x$: il existe un $e \in \{0,1\}$ tel que $\delta_n(x) \equiv (-1)^e 2x \mod 2n+1$.

Nous avons donné dans [Dumas, 2008] une caractérisation complète des quenines (permutations δ_n formant un cycle de longueur n, n est dans ce cas dit **admissible**) :

Théorème 1 ([Dumas, 2008, Théorème 2])**.** *$2n+1$ étant premier, soit $\mathbb{Z}/2n+1\mathbb{Z}$ le corps à $2n+1$ éléments, alors n est admissible si et seulement si :*

- *Soit 2 est d'ordre $2n$ (2 est racine primitive) dans $\mathbb{Z}/2n+1\mathbb{Z}$.*
- *Soit n est impair et 2 est d'ordre n dans $\mathbb{Z}/2n+1\mathbb{Z}$.*

Ainsi, nous pouvons décider facilement si une quenine donnée existe ou non. Suite aux articles de Joerg Arndt [Arndt, 2010, §40.8.2], puis Peter Asveld [Asveld, 2009, §3] nous déduisons la caractérisation suivante, plus précise mais moins pratique à tester. Cette caractérisation est quasiment celle donnée par [Asveld, 2009, Théorème 3.5] ; ce corollaire, que nous (re)démontrons donc en appendice, induit ainsi que [Dumas, 2008, Théorème 2] et [Asveld, 2009, Théorème 3.5] sont bien équivalents.

Corollaire 1. *$2n+1$ étant premier, soit $\mathbb{Z}/2n+1\mathbb{Z}$ le corps à $2n+1$ éléments, alors n est admissible si et seulement si :*

i. $n \equiv 1 \mod 4$ *; +2 est primitif et -2 d'ordre exactement n dans $\mathbb{Z}/2n+1\mathbb{Z}$*

ii. $n \equiv 2 \mod 4$ *; +2 et -2 sont racines primitives dans $\mathbb{Z}/2n+1\mathbb{Z}$*

iii. $n \equiv 3 \mod 4$ *; -2 est primitif et +2 d'ordre exactement n dans $\mathbb{Z}/2n+1\mathbb{Z}$*

*Laboratoire J. Kuntzmann, 51, rue des Mathématiques. Université de Grenoble. UMR CNRS 5224, BP 53X, F38041 Grenoble, France, Jean-Guillaume.Dumas@imag.fr, ljk.imag.fr/membres/Jean-Guillaume.Dumas. Ce travail a été réalisé pour partie alors que l'auteur visitait le ≪ Claude Shannon Institute ≫ et la ≪ School of Mathematical Sciences ≫ de l'≪ University College Dublin ≫, Irlande, en délégation CNRS.

Cette caractérisation s'applique donc également à la caractérisation des entiers pour lesquels des « bases normales optimales de type 2 » existent dans $\mathtt{GF}(2^n)$ [Arndt, 2010, §40.8.2] (voir e.g. [Menezes et al., 1993, Théorème 5.5] pour plus de détails), ainsi qu'à la caractérisation de certains battements de cartes [Asveld, 2009, §3], pour par exemple décrire des synchronisations de processus concurrents (voir e.g. [Jantzen, 1981] pour plus de détails).

Dans la section 2, nous donnons une construction « polynomiale » des quenines : en prenant une racine primitive en $O(\log(n))$, voir [Dumas, 2008, Corollaire 2], nous montrons qu'il suffit de $O(\log^3(n))$ opérations arithmétiques pour trouver tous les rayons de la spirale et leurs orientations. En section 3, nous donnons les correspondances entre les définitions de J. Roubaud et de P. Asveld pour les différentes permutations spirales et introduisons la dernière possibilité de permutation spirale après les quenines, pérecquines et mongines : les roubines. Enfin, en section 4, nous caractérisons les roubines puis en déduisons, en section 5, tous les entiers possédant une permutation spirale généralisée.

2 Orientation des rayons

Les quenines se généralisent, en choisissant une autre racine primitive que 2, à tous les entiers n tels que $2n+1$ est premier. Ainsi, en choisissant le multiplicateur k conformément à [Dumas, 2008, Théorème 5], il est possible de dessiner la permutation comme une spirale avec k rayons sur lesquels nous devons ensuite placer les nombres. Le changement de signe de la congruence induit des changements d'orientation successifs des rayons comme sur la figure 1. Un rayon est dit **sortant** si il est croissant vers l'extérieur de la spirale et **entrant** si il est croissant vers l'intérieur.

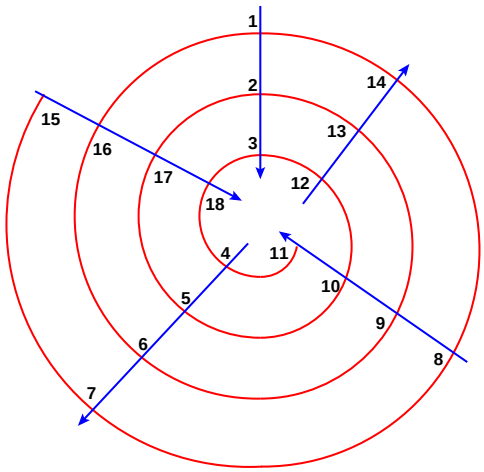

FIGURE 1 – La 5-dixhuitine

En observant l'orientation des rayons sur différentes quenines, comme par exemple sur la figure [Dumas, 2008, Figure 13], reproduite ici, figure 2, il apparaît que les $3,n$-quenines de type 1 (rayon sortant à gauche) sont celles qui vérifient $n \equiv 0 \mod 3$, alors que les $3,n$-quenines de type 2 (rayon sortant à droite) vérifient $n \equiv 2 \mod 3$, comme démontré ci-après.

Lemme 1. *Une $3,n$-quenine a son rayon sortant à gauche si et seulement si $n \equiv 0 \mod 3$. Une $3,n$-quenine a son rayon sortant à droite si et seulement si $n \equiv 2 \mod 3$.*

Démonstration. Considérons $\delta_{n,3}$:

$$\delta_{n,3}(x) \equiv \begin{cases} 3 \cdot x & \text{si } 3x \leq n & \text{entrant} \rightarrow \cdot \\ (2n+1) - 3 \cdot x & \text{si } n+1 \leq 3x \leq 2n & \text{sortant} \leftarrow \cdot \\ -(2n+1) + 3 \cdot x & \text{sinon} & \text{entrant} \rightarrow \cdot \end{cases}$$

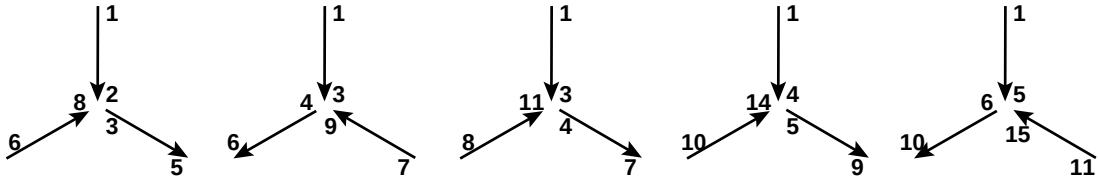

FIGURE 2 – Quelques orientations de $3, n$-quenines

Les rayons de la 3-spirale correspondent aux trois cas possibles dans la définition. En outre, ils sont entrants ou sortants suivant le signe de $3x$ associé.

Par ailleurs, le point de départ de la spirale est par définition $\delta^{-1}(1)$. La question est donc de savoir si $\delta^{-1}(1)$ est sur un rayon entrant ou sortant. Clairement $3x \neq 1$ pour tout $x \in \{1..n/3\}$, donc $\delta^{-1}(1)$ est sur un rayon entrant si et seulement si $\exists x_1$ tel que $-(2n+1)+3\cdot x_1 = 1$. Cela n'est possible que si $3x_1 = 2(n+1)$ autrement dit $2n \equiv -2 \mod 3$ ou encore $n \equiv 2 \mod 3$.

Réciproquement, si $\delta^{-1}(1)$ est sur le rayon sortant, alors $\exists x_1$ tel que $(2n+1)-3\cdot x_1 = 1$ et donc $n \equiv 0 \mod 3$. □

Ceci se généralise à toute racine primitive k, il suffit de chercher les orientations de $\delta^{-1}(i)$ pour $i = 1..(k-1)$, celle du rayon commençant par $1 = \delta^{-1}(k)$ étant entrante par définition.

Sur l'exemple de la figure 1, cela donne donc :

1. $5x_1 \equiv 1 \mod 37$ donne $x_1 = 15$ et $-5x_1 \equiv 1 \mod 37$ donnerait $x_1 = 22 > 18$. Donc le premier rayon commence à 15 et est entrant.
2. $2/5 \equiv 30 \mod 37$ et $2/(-5) \equiv 7 \mod 37$, donc le deuxième rayon commence à 7 et est sortant.
3. $3/5 \equiv 8 \mod 37$ et $3/(-5) \equiv 29 \mod 37$, donc le troisième rayon commence à 8 et est entrant.
4. $4/5 \equiv 23 \mod 37$ et $4/(-5) \equiv 14 \mod 37$, donc le quatrième rayon commence à 14 et est sortant.
5. Le cinquième rayon commence à 1 et est entrant par définition.

Ainsi, il suffit de $2(g-1)$ calculs de pgcd pour déterminer tous les rayons d'une quenine ainsi que leurs orientations, soit de l'ordre de $O(g\log^2(n))$ opérations arithmétiques.

3 Correspondance Roubaud-Asveld

Suivant Roubaud [Roubaud, 2000] ou Audin [Audin, 2009], nous définissons les variantes suivantes de la quenine ou seule l'orientation des rayons change. Avec deux rayons, il y a quatre couples d'orientations possibles pour des permutations de type spirale :

- Entrant-Sortant : il s'agit des quenines.
- Entrant-Entrant : ce sont les pérecquines, d'après [Dumas, 2008, §9].
- Sortant-Entrant : ce sont les mongines, car elles correspondent à des battements de cartes de G. Monge.
- Sortant-Sortant : nous proposons de les appeler **roubines** [1].

Par ailleurs, il est possible de renverser complètement les permutations obtenues pour obtenir quatre nouvelles permutations. Si nécessaire nous noterons d'un indice 0 la permutation initiale et d'un indice 1 la permutation renversée, comme sur la figure 3.

Les quenines-1 et les pérecquines-1 laissant 1 invariant ne peuvent donner des cycles de longueur n, nous les laisserons donc de côté.

1. Une roubine ou *robine* est également un petit canal de communication d'un étang salé avec la mer ; les roubines noires ou *terres noires* sont des marnes sombres présentes dans les alpes du sud.

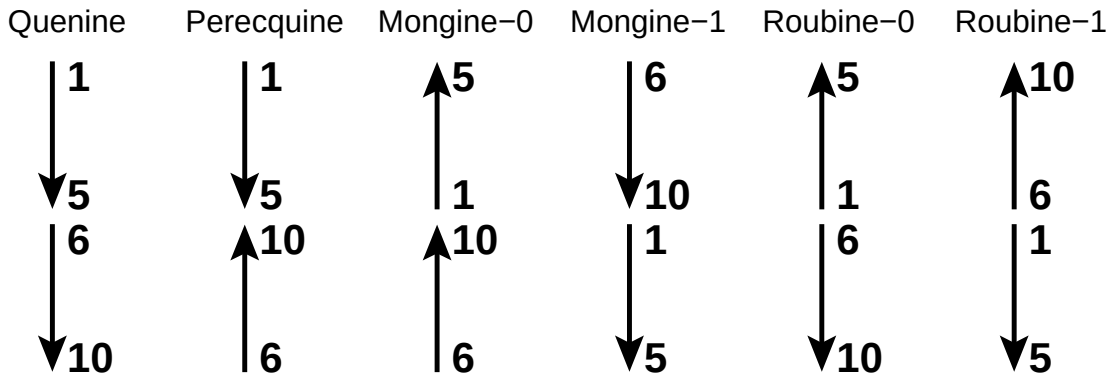

FIGURE 3 – Quenine, pérecquine, mongine et roubine de taille 10

Dans la table 1, nous donnons les correspondances entre ces permutations et celles issues de battements de cartes décrites dans [Asveld, 2009]. Pour les trois premiers cas, la correspondance est exacte et les caractérisations sont données dans [Dumas, 2008] et [Asveld, 2009]. Dans la table 2, nous explicitons le cas de la roubine : il faut distinguer n pair de n impair ce qui avec les indices 0 et 1 donne 4 fonctions de définition des permutations, S' et $\overline{S'}$, qui correspondent à nos roubine-0 et roubine-1 de manière croisée.

Spirale P. Asveld	Quenine Twist	Pérecquine Perfect Shuffle	Mongine-0 Archimedes-0	Mongine-1 Archimedes-1
Permutation	$\delta \equiv (-1)^e 2m \ [n+1]$	$\pi \equiv 2m \ [n+1]$	$\mu_0 = \lceil \frac{n+1}{2} \rceil + (-1)^{m-1} \lceil \frac{m-1}{2} \rceil$	$\mu_1 = \lceil \frac{n}{2} \rceil + (-1)^{m} \lceil \frac{m-1}{2} \rceil$

TABLE 1 – Correspondances entre permutations spirales et Asveld

	n pair		n impair	
Spirale P. Asveld	Roubine-0 S'	Roubine-1 $\overline{S'}$	Roubine-0 $\overline{S'}$	Roubine-1 S'
Permutation	$\rho_{0p} = \begin{cases} n+2-2m \\ 2n+1-2m \end{cases}$	$\rho_{1p} \equiv -2x \ [n+1]$	$\rho_{0i} \equiv 1-2x \ [n]$	$\rho_{1i} \equiv 2-2x \ [n]$

TABLE 2 – Correspondances entre roubines et Asveld

Ainsi, nous pouvons donner des caractérisations pour les trois premières familles :

1. Quenines : i., ii. ou iii. du corollaire 1.
2. Pérecquine : si et seulement si 2 est racine primitive modulo $2n+1$ [Dumas, 2008, Th. 7].
3. Mongine-0 : si et seulement si n est pair et (ii.) [Asveld, 2009, Th. 4.3].
4. Mongine-1 : si et seulement si n est impair et (i. ou iii.) [Asveld, 2009, Th. 4.3].

Il reste donc à déterminer la caractérisation des roubines. Celle-ci est l'objet des deux derniers points de la conjecture [Asveld, 2009, Conj. 7.2], que nous démontrons ci-après.

4 L'ordre des roubines

Nous montrons d'abord la correspondance entre les formules de la table 2 et les définitions de [Asveld, 2009, §7.4].

Lemme 2. *Les formules des roubines de la table 2 sont correctes.*

Démonstration. Pour n donné, [Asveld, 2009, §7.4] définit $\overline{k} = \lceil \frac{n+1}{2} \rceil$ et $k = \lceil \frac{n}{2} \rceil$. Si n est impair alors $2\overline{k} = 2k = n + 1$ et

$$p(\overline{S'}, n) = \rho_{0i} = \begin{cases} n + 1 - 2m & \text{si } 1 \leq m < k \\ n - 2(m-k) = n - 2m + n + 1 & \text{sinon} \end{cases} \equiv 1 - 2m \mod n$$

ainsi que

$$p(S', n) = \rho_{1i} = \begin{cases} n + 2 - 2m & \text{si } 1 \leq m < k \\ n + 1 - 2(m-k) = n + 1 - 2m + n + 1 & \text{sinon} \end{cases} \equiv 2 - 2m \mod n.$$

De la même manière, si n est pair alors $2\overline{k} = n + 2$, mais $2k = n$ et

$$p(\overline{S'}, n) = \rho_{1p} = \begin{cases} n + 1 - 2m & \text{si } 1 \leq m < k \\ n - 2(m-k) = n - 2m + n + 2 & \text{sinon} \end{cases} \equiv -2m \mod (n+1)$$

ainsi que

$$p(S', n) = \rho_{0p} = \begin{cases} n + 2 - 2m & \text{si } 1 \leq m < k \\ n + 1 - 2(m-k) = n + 1 - 2m + n & \text{sinon} \end{cases}.$$

□

Avec ces congruences il est ensuite aisé de conclure sur la conjecture [Asveld, 2009, Conj. 7.2].

Théorème 2. *1. ρ_{0p} est d'ordre n si et seulement si $n = 2$.*

2. ρ_{0i} est d'ordre n si et seulement si $n = 3^k$.

3. ρ_{1p} est d'ordre n si et seulement si -2 est racine primitive de $n + 1$.

4. ρ_{1i} est d'ordre n si et seulement si $n = 3^k$.

Démonstration. On utilise la caractérisation suivante des générateurs congruentiels linéaires [Knuth, 1997, Théorème 3.2.1.2.A] : un générateur $X_{n+1} = aX_n + c \mod n$ est d'ordre n si et seulement si $pgcd(c, n) = 1$, $a - 1$ est divisible par tous les facteurs premiers de n et $a - 1$ est un multiple de 4 si n est un multiple de 4.

1. $\rho_{0p}(1) = n$ et $\rho_{0p}(n) = 1$ donc l'orbite de 1 est de taille 2.
2. ρ_{0i} est un générateur congruentiel linéaire. Ainsi, il est d'ordre n si et seulement si 1 est premier avec n et les diviseurs de n divisent également $a - 1 = -2 - 1 = n - 3$, donc si et seulement si $n = 3^k$.
3. la preuve est identique à celle des pérecquines [Dumas, 2008, Th. 7].
4. ρ_{1i} est un générateur congruentiel linéaire. Ainsi, il est d'ordre n si et seulement si 2 est premier avec n impair et les diviseurs de n divisent également $a - 1 = -2 - 1 = n - 3$, donc si et seulement si $n = 3^k$.

□

Il s'avère donc que la roubine-1 est plus intéressante que la roubine-0, nous la noterons donc dorénavant simplement roubine. Les figures 4 et 5 montrent les roubines pour $n = 6$ et $n = 9$, d'ordre n, et la table 3 donne les les roubines inférieures à 2500.

Bien sûr, les roubines se généralisent pour tout multiplicateur : dans le cas où n est pair, à tout multiplicateur g dont $-g$ est racine primitive de $n + 1$; dans le cas impair, pour tout $n = p_1^{a_1} \dots p_j^{a_j}$, à tout multiplicateur $g = p_1^{\alpha_1} \dots p_j^{\alpha_j} - 1$ tel que $\alpha_i \geq 1$ pour tout i. Il s'en suit que tous les nombres impairs peuvent s'écrire sous la forme d'une roubine : en prenant par exemple $g = n - 1$ on obtient $\delta = 2 - gx \equiv 2 + x \mod n$ qui est bien d'ordre n. Cette dernière roubine n'est cependant pas très intéressante puisqu'elle possède $n - 1$ rayons ! Les roubines avec au moins deux éléments par rayon sont plus jolies, il s'agit des n multiples d'au moins un carré, car ainsi on peut prendre $g < n/2$. Les figures 6 et 7 présentent respectivement une roubine paire de multiplicateur 3 et une roubine impaire de multiplicateur 4.

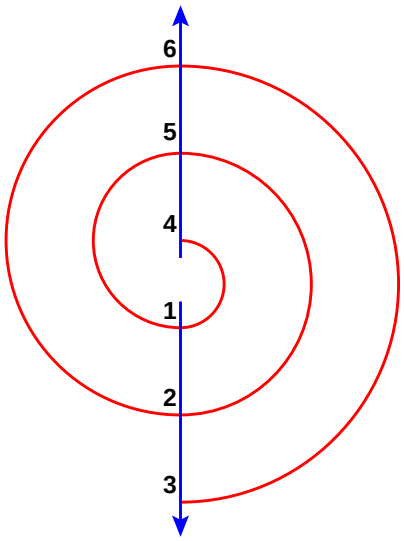

FIGURE 4 – La 6-roubine

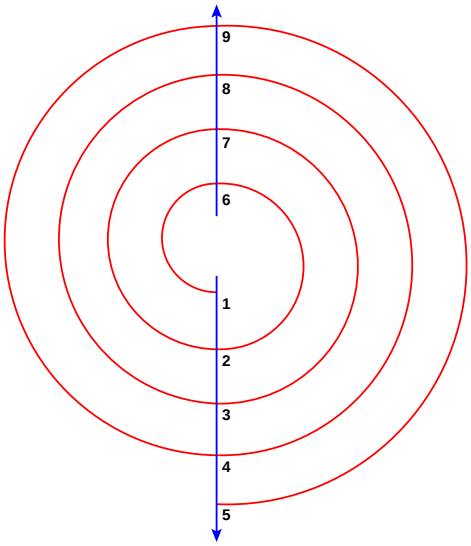

FIGURE 5 – La 9-roubine

1	3	4	6	9	12	22	27	28	36	46	52	60	70
78	81	100	102	148	166	172	180	190	196	198	238	243	262
268	270	292	310	316	348	358	366	372	382	388	420	460	462
478	486	502	508	540	556	598	606	612	646	652	660	676	700
708	718	729	742	750	756	772	796	820	822	828	838	852	862
876	886	940	966	982	990	1030	1038	1060	1062	1086	1108	1116	1150
1212	1222	1228	1230	1236	1276	1278	1300	1302	1318	1366	1372	1380	1438
1446	1452	1486	1492	1510	1542	1548	1558	1566	1582	1606	1620	1636	1662
1668	1692	1732	1740	1758	1782	1822	1846	1860	1870	1876	1878	1900	1948
1950	1972	1996	2028	2038	2052	2062	2068	2086	2110	2140	2187	2206	2212
2220	2236	2238	2268	2292	2308	2310	2332	2356	2388	2398	2422	2436	2446
2476													

TABLE 3 – Les roubines inférieures à 2500

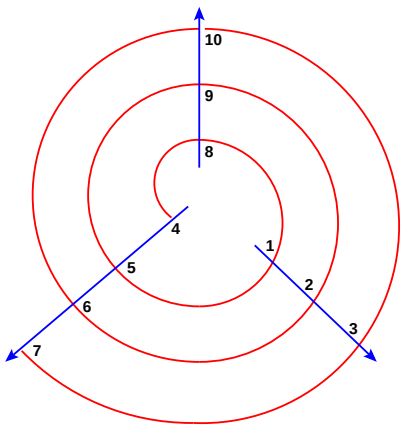

FIGURE 6 – La 10-roubine de multiplicateur 3

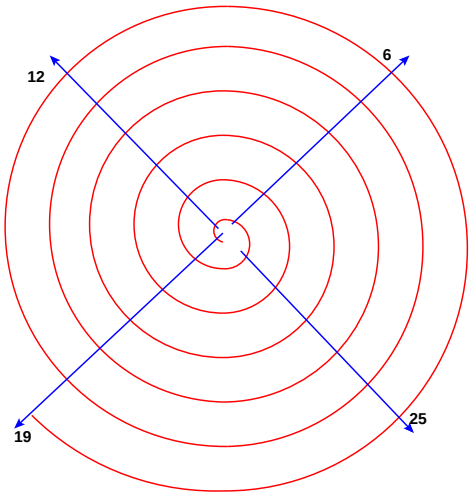

FIGURE 7 – La 25-roubine de multiplicateur 4

5 Les spinines

Avec les roubines, et plus précisément, les générateurs congruentiels, l'ensemble des entiers possédant une permutation spirale s'est considérablement agrandi. Aux n tels que $2n+1$ soit premier (avec les quenines, les mongines) et tels que $n+1$ soit premier (pérecquines, roubines), on ajoute au moins les entiers impairs divisibles par un carré, et même tous les entiers impairs, si l'on s'autorise les roubines à $n-1$ rayons. Cela induit donc l'idée d'une généralisation aux entiers pairs, par un générateur congruentiel. Afin de pouvoir obtenir des permutations d'ordre maximal, il faudra additionner un élément c premier avec n, choisissons donc $c=1$, et un multiplicateur a tel que les diviseurs premiers de n, et 4 si celui-ci divise n, divisent également $a-1$. On obtient alors la définition 1 qui permet d'obtenir une permutation spirale pour tout n.

Définition 1. *Soient $n \in \mathbb{N}$ et g premier avec n. La n-spinine de multiplicateur g, ou n,g-spinine, est la permutation de $1..n$ dans $1..n$ vérifiant $\gamma_{n,g}(m) \equiv 1 - g \cdot m \mod n$.*

Théorème 3. *Une n,g-spinine est d'ordre n si et seulement si tous les diviseurs premiers de n divisent $g+1$ et si $g+1$ est un multiple de 4 quand n l'est aussi.*

De même que pour les roubines, les rayons des spinines sont uniquement sortants et comme pour les constructions précédentes, les valeurs finales sont les images réciproques de $1..g$ par $\gamma_{n,g}$. Les figures 8 et 9 montrent des spinines d'ordre n. La figure 9 est à comparer avec la roubine de mêmes paramètres, figure 7.

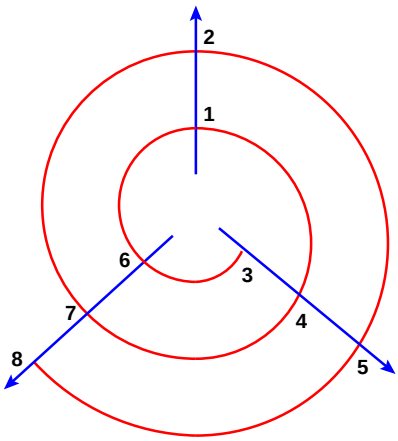

FIGURE 8 – La 8-spinine de multiplicateur 3

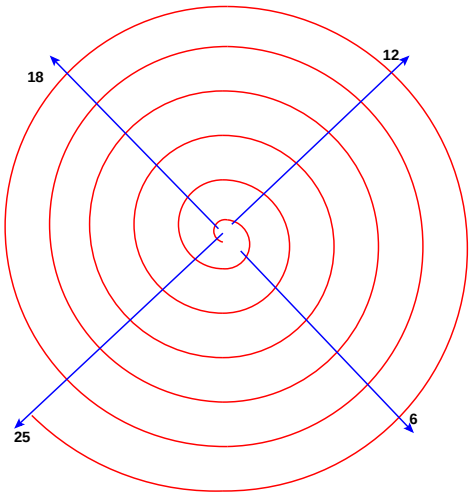

FIGURE 9 – La 25-spinine de multiplicateur 4

6 Conclusion

En combinant les quenines ($2n+1$ premier tout comme les mongines), les pérecquines ($n+1$ premier tout comme certaines roubines), les roubines, et surtout les spinines (pour tout n), tous les entiers possèdent dorénavant au moins une permutation spirale. Néanmoins, quand n est sans carré, les roubines impaires et les spinines nécessitent d'avoir $n-1$ rayons d'après le théorème 3. Leur esthétique est donc assez réduite. On parlera alors de **jolie** spinine quand n possède un carré et plus généralement de **jolie** permutation spirale quand $2n+1$ ou $n+1$ est premier ou quand n possède un carré. Celles-ci possèdent au plus $n/2$ rayons et chaque rayon comporte au moins deux éléments. Il reste tout de même assez peu d'entiers ne possédant pas de jolie permutation spirale, la table 4 recense ceux inférieurs à 1000.

7	13	17	19	31	34	37	38	43	47	55	57	59	61
62	67	71	73	77	79	85	87	91	93	94	97	101	103
107	109	110	115	118	122	123	127	129	133	137	139	142	143
145	149	151	154	157	159	161	163	167	170	177	181	182	185
187	193	195	197	199	201	202	203	205	206	211	213	214	217
218	223	227	229	235	237	241	246	247	253	255	257	258	259
263	265	266	267	269	271	274	277	283	286	287	290	291	295
298	301	302	305	307	311	313	314	317	318	319	322	327	331
334	335	337	339	347	349	353	355	357	362	365	367	370	373
374	377	379	381	383	385	389	390	391	394	395	397	399	401
402	403	406	407	409	415	417	421	422	427	433	434	435	437
439	445	446	447	449	451	454	457	458	461	463	465	467	469
471	474	479	481	482	487	489	493	494	497	499	501	503	505
511	514	517	518	521	523	526	527	533	535	537	538	541	542
547	553	555	557	559	563	565	566	569	571	573	574	577	579
582	583	587	589	591	595	597	599	601	602	607	609	610	613
617	619	622	623	626	627	631	633	634	635	643	647	649	654
655	661	662	665	667	669	670	671	673	674	677	678	679	681
685	687	689	691	694	695	697	698	701	703	705	706	707	709
710	715	717	721	727	730	731	733	734	737	739	745	751	753
754	757	758	759	762	763	766	767	769	770	773	777	778	781
782	787	790	793	794	795	797	799	802	805	807	811	814	815
817	821	823	827	829	830	835	839	842	843	851	853	857	859
863	865	869	871	874	877	878	881	883	885	887	889	890	895
897	898	899	901	902	903	907	913	914	917	919	921	922	926
929	934	937	941	942	943	947	949	951	955	957	958	959	962
967	969	971	973	977	978	979	983	985	987	991	994	995	997

TABLE 4 – Entiers inférieurs à 1000 ne possédant pas de jolie permutation spirale

Comme la densité des entiers sans carré est asymptotiquement $Q(n) = \frac{6n}{\pi^2} + O(\sqrt{n})$ d'après [Hardy and Wright, 2008, Théorème 333] un peu plus de 60% des entiers possèdent donc de jolies permutations spirales.

Références

[Arndt, 2010] Arndt, J. (2010). *Matters Computational*. http ://www.jjj.de/fxt/#fxtbook, to appear.

[Asveld, 2009] Asveld, P. R. J. (2009). Permuting operations on strings : Their permutations and their primes. Technical report, TR-CTIT-09-26, Centre for Telematics and Information Technology, University of Twente, Enschede.

[Audin, 2007] Audin, M. (2007). Mathématiques et littérature. *Mathématiques et sciences humaines*, 178 :63–86.

[Audin, 2009] Audin, M. (2009). Poésie, spirales, et battements de cartes. *Images des Mathématiques*, 18. `http://images.math.cnrs.fr/Poesie-spirales-et-battements-de.html`.

[Bach and Shallit, 1996] Bach, E. and Shallit, J. (1996). *Algorithmic Number Theory : Efficient Algorithms*. MIT press.

[Dumas, 2008] Dumas, J.-G. (2008). Caractérisation des quenines et leur représentation spirale. *Mathématiques et Sciences Humaines*, 4(184) :9 – 23.

[Hardy and Wright, 2008] Hardy, G. H. and Wright, E. M. (2008). *An Introduction to the Theory of Numbers*. Oxford University Press, sixth edition.

[Jantzen, 1981] Jantzen, M. (1981). The power of synchronizing operations on strings. *Theoretical Computer Science*, 14(2) :127–154.

[Knuth, 1997] Knuth, D. E. (1997). *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, USA, 2^{nd} edition.

[Menezes et al., 1993] Menezes, A. J., Blake, I. F., Gao, X., Mullin, R. C., Vanstone, S. A., and Yaghoobian, T. (1993). *Applications of Finite Fields*. Kluwer Academic Publishers.

[Roubaud, 2000] Roubaud, J. (2000). Réflexions historiques et combinatoires sur la n-ine autrement dit quenine. *La bibliothèque Oulipienne*, 5(66) :99–124. Contribution à la réunion 395 de l'Oulipo, le 17 septembre 1993.

A Preuve du corollaire 1

Nous devons démontrer que $2n+1$ étant premier, soit $\mathbb{Z}/_{2n+1}\mathbb{Z}$ le corps à $2n+1$ éléments, alors n est admissible si et seulement si :

i. $n \equiv 1 \mod 4$; +2 est primitif et -2 d'ordre exactement n dans $\mathbb{Z}/_{2n+1}\mathbb{Z}$

ii. $n \equiv 2 \mod 4$; +2 et -2 sont racines primitives dans $\mathbb{Z}/_{2n+1}\mathbb{Z}$

iii. $n \equiv 3 \mod 4$; -2 est primitif et +2 d'ordre exactement n dans $\mathbb{Z}/_{2n+1}\mathbb{Z}$

Démonstration. La caractérisation du corollaire contient celle du théorème 1 (si $n \equiv 1$ ou 2 alors 2 est d'ordre $2n$, et si $n \equiv 3$ alors n est impair et 2 est d'ordre n), il suffit donc de démontrer la réciproque. Pour cela, il faut démontrer les points suivants :

i. 2 est d'ordre $2n$ est incompatible avec $n \equiv 0 \mod 4$ ou $n \equiv 3 \mod 4$.

ii. 2 est d'ordre n est incompatible avec $n \equiv 1 \mod 4$.

iii. -2 est d'ordre n quand $n \equiv 1 \mod 4$.

iv. -2 est d'ordre $2n$ quand $n \equiv 2 \mod 4$.

v. -2 est d'ordre $2n$ et 2 est d'ordre n quand $n \equiv 3 \mod 4$.

Le caractère de résiduïcité de 2 (voir par exemple [Bach and Shallit, 1996, Théorème 5.8.1]) nous donne plusieurs réponses et le reste se déduit simplement :

i. Si $n \equiv 0 \mod 4$ (resp. $n \equiv 3 \mod 4$) alors $2n+1 \equiv 1 \mod 8$ (resp. $2n+1 \equiv 7 \mod 8$) et donc dans les deux cas 2 est un résidu quadratique modulo $2n+1$. Ce qui implique que l'ordre de 2 ne peut donc pas être maximal $2n$, mais seulement inférieur ou égal à n.

ii. Au contraire, si $n \equiv 1 \mod 4$ alors $2n+1 \equiv 3 \mod 8$ et donc dans cas 2 n'est pas un résidu quadratique modulo $2n+1$. Supposons alors que l'ordre de 2 est n. Il s'en suit que $2^n \equiv 1$ ou encore $2^{4k+1} \equiv 1$. Cela implique que $2^{4k+2} \equiv \left(2^{2k+1}\right)^2 \equiv 2$ et donc 2 serait un résidu quadratique ce qui est absurde.

iii. Le point précédent et le théorème 1 montrent que lorsque $n \equiv 1 \mod 4$, 2 est d'ordre $2n$. Alors $2^n \equiv -1$ et donc $(-2)^n \equiv (-1)^n \times 2^n \equiv 1$ car n est impair. Ainsi, e l'ordre de -2 vérifie $e \leq n$ et $(-2)^e \equiv 1$. Cette dernière équation implique que $2^{2e} = ((-2)^e)^2 \equiv 1$ et donc que $2n$, l'ordre de 2, vérifie $2n|2e$, combiné à $e \leq n$, on obtient $e = n$.

iv. Soit e l'ordre de -2, encore une fois $2^{2e} \equiv 1$. Si $n \equiv 2 \mod 4$ alors le théorème 1 prouve que 2 est d'ordre $2n$ et donc $2n|2e$, soit $e = n$ ou $e = 2n$. Comme 2 est primitif, on a également $2^n \equiv -1$, ou encore comme n est pair, $(-2)^n \equiv -1$ et donc $e \neq n$.

v. Le premier point ci-dessus et le théorème 1 montrent que 2 est forcément d'ordre n quand $n \equiv 3 \mod 4$. Soit e l'ordre de -2, encore une fois $2^{2e} \equiv 1$ et donc $n|2e$. Cette fois-ci, n est impair et donc $n|e$, de sorte que $e = n$ ou $e = 2n$; dans les deux cas $2^e \equiv 1$. Mais comme e est l'ordre de -2, alors $1 \equiv (-2)^e = (-1)^e \times 2^e$, donc e est forcément pair et donc $e = 2n$.

□