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, ci-après dénommée Roubine en l'honneur de ce dernier. Enfin nous démontrons la conjecture [Asveld, 2009, Conjecture 7.2].

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

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 cyle 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, 2009, §40.8.2], puis Peter Asveld [Asveld, 2009, §3] nous déduisons la caractérisation suivante, plus précise mais du coup moins pratique à tester. Cette caractérisation est quasiment celle donnée par [Asveld, 2009, Théorème 3.5] ; nous (re)démontrons donc ici 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.

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 :

1. 2 est d'ordre $2n$ est incompatible avec $n \equiv 0 \mod 4$ ou $n \equiv 3 \mod 4$.
2. 2 est d'ordre n est incompatible avec $n \equiv 1 \mod 4$.
3. -2 est d'ordre n quand $n \equiv 1 \mod 4$.
4. -2 est d'ordre $2n$ quand $n \equiv 2 \mod 4$.
5. -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 :

1. 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.
2. 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.
3. 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 $e = n$.
4. 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 $e \neq n$.
5. 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 $e = 2n$.

□

Cette caractérisation peut alors directement s'appliquer à la caractérisation des entiers pour lesquels des « bases normales optimales de type 2 » existent dans $\mathtt{GF}(2^n)$ [Arndt, 2009, §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 et en déduisons 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 changement 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.

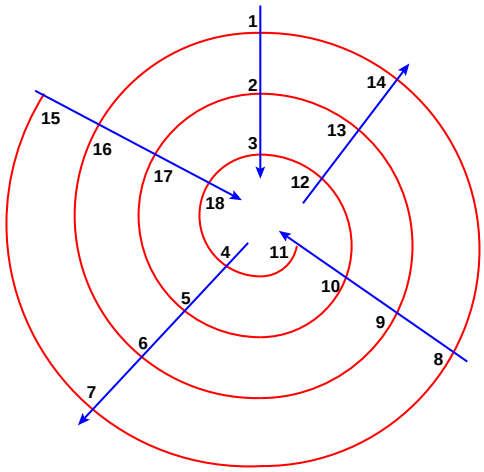

FIGURE 1 – La 5-dixhuitine

En observant l'orientation des rayons sur différentes quenines, comme par exemple sur la figure [Dumas, 2008, Figure 13], reproduite ici, figure 2, il apparait 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.

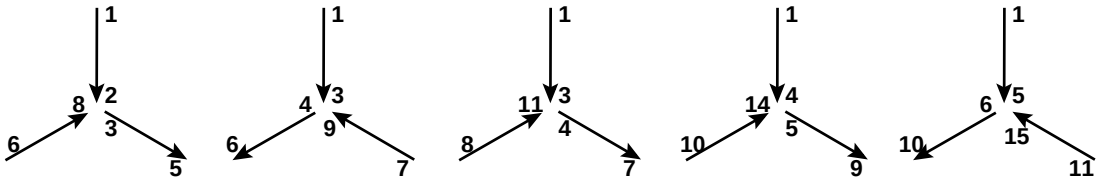

FIGURE 2 – Quelques orientations de $3, n$-quenines

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 $\delta_{n,3}$:

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

Les rayons de la 3-spirale correspondents 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.

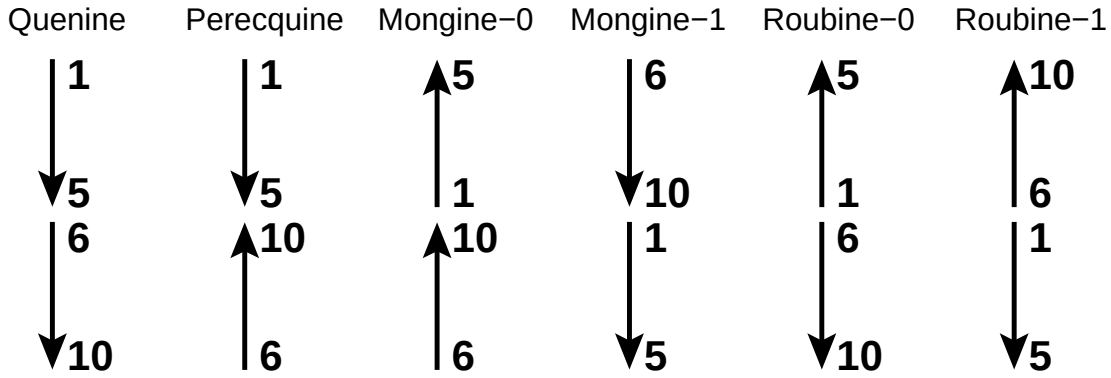

FIGURE 3 – Quenine, Pérecquine, Mongine et Roubine de taille 10

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

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.

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	$\gamma_{0p} = \begin{cases} n+2-2m \\ 2n+1-2m \end{cases}$	$\gamma_{1p} \equiv -2x[n+1]$	$\gamma_{0i} \equiv 1-2x[n]$	$\gamma_{1i} \equiv 2-2x[n]$

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

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

ainsi que

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

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

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

ainsi que

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

□

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

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

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

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

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

Démonstration. On utilise la caractérisation suivante des générateurs congruentiels linéaires [Knuth, 1997, pp 17-19] : 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. $\gamma_{0p}(1) = n$ et $\gamma_{0p}(n) = 1$ donc l'orbite de 1 est de taille 2.
2. γ_{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. γ_{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.

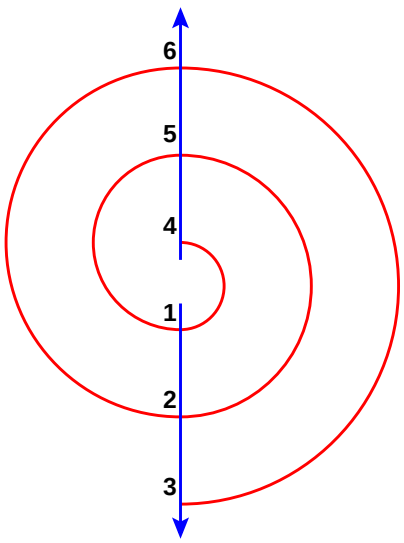

FIGURE 4 – La 6-roubine

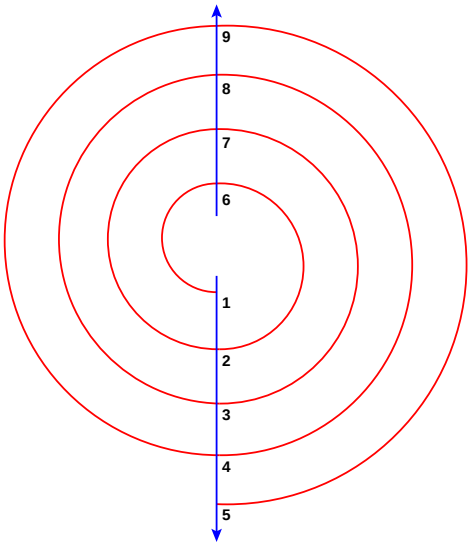

FIGURE 5 – La 9-roubine

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

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

$n = p_1^{a_1} \dots p_j^{a_j}$, 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.

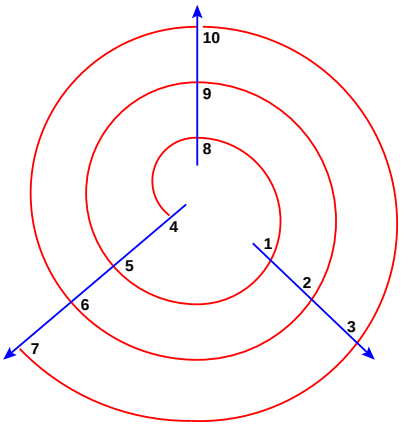

FIGURE 6 – La 10-roubine de multiplicateur 3

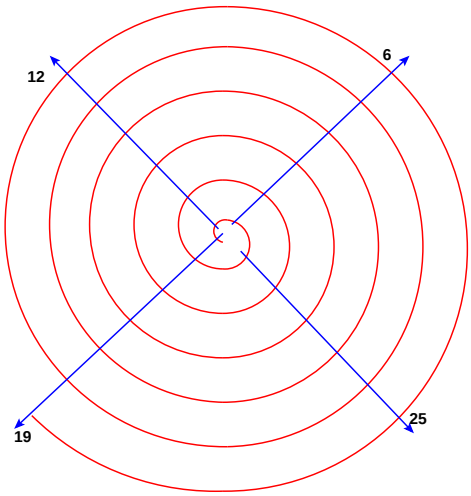

FIGURE 7 – La 25-roubine de multiplicateur 4

5 Conclusion

Avec les roubines l'ensemble des entiers possédant une permuation 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. Les roubines paires ou impaires possédant un carré seront appelées **roubines pures**, la table 4 donne celles inférieures à 1000.

Il reste alors assez peu d'entiers non pourvu d'une permutation spirale, il s'agit des entiers pairs tels que ni $n + 1$, ni $2n + 1$ n'est premier. La table 5 donne ceux inférieurs à 1000

1	2	4	6	9	10	12	16	18	22	25	27	28	30
36	40	42	45	46	49	52	58	60	63	66	70	72	75
78	81	82	88	96	99	100	102	106	108	112	117	121	125
126	130	135	136	138	147	148	150	153	156	162	166	169	171
172	175	178	180	189	190	192	196	198	207	210	222	225	226
228	232	238	240	243	245	250	256	261	262	268	270	275	276
279	280	282	289	292	297	306	310	312	315	316	325	330	333
336	343	346	348	351	352	358	361	363	366	369	372	375	378
382	387	388	396	400	405	408	418	420	423	425	430	432	438
441	442	448	456	459	460	462	466	475	477	478	486	490	495
498	502	507	508	513	520	522	525	529	531	539	540	546	549
556	562	567	568	570	575	576	585	586	592	598	600	603	605
606	612	616	618	621	625	630	637	639	640	642	646	652	657
658	660	672	675	676	682	690	693	700	708	711	718	725	726
729	732	735	738	742	747	750	756	760	765	768	772	775	783
786	796	801	808	810	819	820	822	825	826	828	833	837	838
841	845	847	852	855	856	858	862	867	873	875	876	880	882
886	891	906	909	910	918	925	927	928	931	936	940	945	946
952	961	963	966	970	975	976	981	982	990	996	999		

TABLE 4 – Les g-roubines pures inférieures à 1000

24	32	34	38	62	64	76	80	84	92	94	104	110	118
122	124	132	142	144	152	154	160	164	170	182	184	188	202
206	208	212	214	218	220	234	236	242	244	246	248	252	258
264	266	272	274	286	290	294	298	302	304	314	318	322	324
328	332	334	340	342	344	356	360	362	364	368	370	374	376
390	392	394	402	406	412	416	422	424	434	436	444	446	450
452	454	458	472	474	480	482	484	492	494	496	500	512	514
518	526	528	532	536	538	542	544	550	552	560	566	572	574
578	580	582	584	588	594	602	604	610	620	622	626	628	632
634	636	654	656	662	664	666	668	670	674	678	684	688	692
694	696	698	702	706	710	712	720	722	724	728	730	734	736
748	752	754	758	762	764	766	770	778	780	782	784	788	790
792	794	802	812	814	816	824	830	832	836	840	842	844	850
864	868	872	874	878	884	890	892	896	898	902	904	908	912
914	916	920	922	924	926	932	934	942	948	954	958	960	962
964	968	972	978	980	984	988	992	994					

TABLE 5 – Entiers non spiraliques inférieurs à 1000

Références

[Arndt, 2009] Arndt, J. (2009). Algorithms for programmers. 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. *Mathematics and Social Sciences*, 4(184) :9 – 23.

[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*. Addison-Wesley, Reading, MA, USA.

[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.