



# Les rayons des permutations spirales

Jean-Guillaume Dumas

## ► To cite this version:

| Jean-Guillaume Dumas. Les rayons des permutations spirales. 2010. hal-00447415v3

**HAL Id: hal-00447415**

**<https://hal.science/hal-00447415v3>**

Preprint submitted on 28 Jan 2010 (v3), last revised 23 Feb 2010 (v5)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# 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 battements de cartes définis par [Asveld, 2009] et les quenines, pérecquines, mongines de Jacques Roubaud, ainsi que la quatrième variante possible, ici dénommée roubine. Ensuite, nous démontrons la conjecture [Asveld, 2009, Conjecture 7.2], en reliant les permutations spirales aux générateurs congruents linéaires. Enfin nous en déduisons une définition générale et des constructions de permutations spirales pour tout entier.

Oh la jolie 3-septine ordonnée sortante : [7<-5 4<-3 2<-1]

## Summary

We give a new characterization of quenines and prove the conjecture of [Dumas, 2008] on spiral rays orientation. We give relations between the shuffles of [Asveld, 2009] and the quenines, pérecquines, mongines of Jacques Roubaud, together with the fourth possible variante, the roubine. Then we prove the conjecture [Asveld, 2009, Conjecture 7.2] by relating spiral permutations to linear congruential generators. Finally we propose a definitions and constructions of spiral permutations for any integer.

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

## 1 Introduction

Nous considérons la permutation  $\delta_n$  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  $\delta_n(x) \equiv (-1)^e 2x \pmod{2n+1}$ .

Nous avons donné dans [Dumas, 2008] une caractérisation complète des quenines (permutations  $\delta_n$  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  $\mathbb{Z}/2n+1\mathbb{Z}$ .*

---

\*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.

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 annexe, 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.  $n \equiv 1 \pmod{4}$  ;  $+2$  est primitif et  $-2$  d'ordre exactement  $n$  dans  $\mathbb{Z}/2n+1\mathbb{Z}$
- ii.  $n \equiv 2 \pmod{4}$  ;  $+2$  et  $-2$  sont racines primitives dans  $\mathbb{Z}/2n+1\mathbb{Z}$
- iii.  $n \equiv 3 \pmod{4}$  ;  $-2$  est primitif et  $+2$  d'ordre exactement  $n$  dans  $\mathbb{Z}/2n+1\mathbb{Z}$

Cette caractérisation s'applique donc également à la caractérisation des entiers pour lesquels des « bases normales optimales de type 2 » existent dans  $\mathbf{GF}(2^n)$  [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 stricte permutation spirale après les quenines, pérecquines et mongines : les roubines. Ensuite, en section 4, nous caractérisons les roubines, par des techniques de générateurs congruentiels linéaires, puis en déduisons, en section 5, la spiruline, permutation spirale pour tout entier. Enfin, en section 6, nous classifions les notions de jolie permutation spirale, de permutations spirales ordonnées, entrantes ou sortantes, grâce à leurs rayons. Ceci donne une alternative graphique aux spirales pour la construction générale de permutations spirales.

## 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.

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  $n \equiv 0 \pmod{3}$ , alors que les  $3, n$ -quenines de type 2 (rayon sortant à droite) vérifient  $n \equiv 2 \pmod{3}$ , comme démontré ci-après.

**LEMME 1.** *Une  $3, n$ -quenine a son rayon sortant à gauche si et seulement si  $n \equiv 0 \pmod{3}$ .*

*Une  $3, n$ -quenine a son rayon sortant à droite si et seulement si  $n \equiv 2 \pmod{3}$ .*

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

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

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

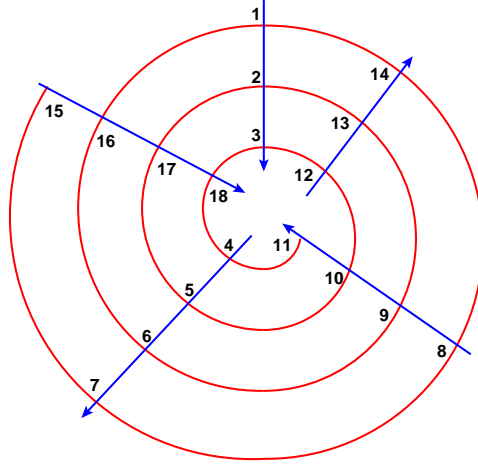


FIGURE 1 – La 5-dixhuitine

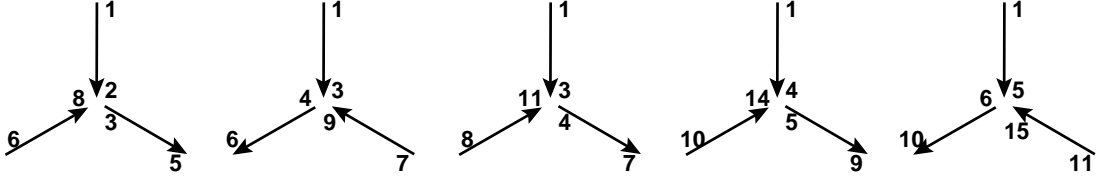


FIGURE 2 – Quelques orientations de 3,  $n$ -quenines

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  $\exists r_1$  tel que  $-(2n+1) + 3 \cdot r_1 = 1$ . Cela n'est possible que si  $3r_1 = 2(n+1)$  autrement dit  $2n \equiv -2 \pmod{3}$  ou encore  $n \equiv 2 \pmod{3}$ .

Réciproquement, si  $\delta^{-1}(1)$  est sur le rayon sortant, alors  $\exists r_1$  tel que  $(2n+1) - 3 \cdot r_1 = 1$  et donc  $n \equiv 0 \pmod{3}$ .  $\square$

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.  $5r_1 \equiv 1 \pmod{37}$  donne  $r_1 = 15$  et  $-5r_1 \equiv 1 \pmod{37}$  donnerait  $r_1 = 22 > 18$ . Donc le premier rayon commence à 15 et est entrant.
2.  $2/5 \equiv 30 \pmod{37}$  et  $2/(-5) \equiv 7 \pmod{37}$ , donc le deuxième rayon commence à 7 et est sortant.
3.  $3/5 \equiv 8 \pmod{37}$  et  $3/(-5) \equiv 29 \pmod{37}$ , donc le troisième rayon commence à 8 et est entrant.
4.  $4/5 \equiv 23 \pmod{37}$  et  $4/(-5) \equiv 14 \pmod{37}$ , 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 d'un calcul de pgcd pour déterminer  $g^{-1} \pmod{2n+1}$ , puis d'au plus  $g-1$  multiplications et additions modulaires pour déterminer tous les rayons d'une quinine ainsi que leurs orientations, soit de l'ordre de  $O(g \log^2(n))$  opérations arithmétiques.

Cela nous donne donc la procédure générale 1, probabiliste et polynomiale, pour déterminer les quenines.



**DÉFINITION 1.** Une permutation est dite **spirale** si et seulement si, quand les entiers qui la composent sont écrits sur une spirale, ceux se situant à un même angle (sur un même rayon) sont consécutifs.

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].

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

TABLE 1 – Correspondances entre permutations spirales et Asveld

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

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

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

ainsi que

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

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

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

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.  $\rho_{0p}$  est d'ordre  $n$  si et seulement si  $n = 2$ .

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

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

4.  $\rho_{1i}$  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  $X_{n+1} = aX_n + c \pmod{n}$  est d'ordre  $n$  si et seulement si  $\text{pgcd}(c, n) = 1$ ,  $a - 1$  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.  $\rho_{0i}$  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.  $\rho_{1i}$  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.

|      |      |      |      |      |      |      |      |      |      |      |      |      |      |
|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| 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

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  $n = p_1^{\alpha_1} \dots p_j^{\alpha_j}$ , 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

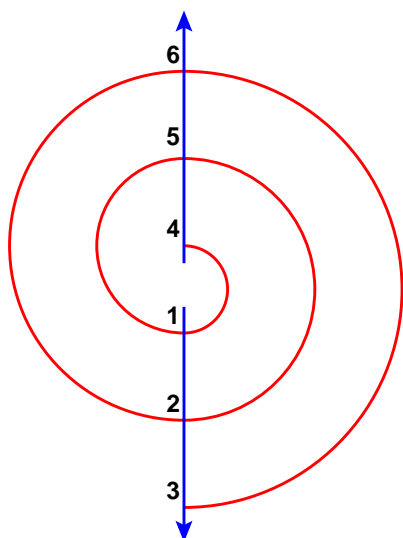


FIGURE 4 – La 6-roubine

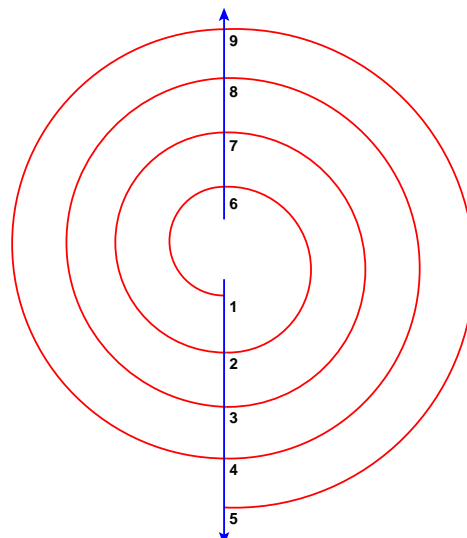


FIGURE 5 – La 9-roubine

exemple  $g = n - 1$  on obtient  $\delta = 2 - gx \equiv 2 + x \pmod{n}$  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.

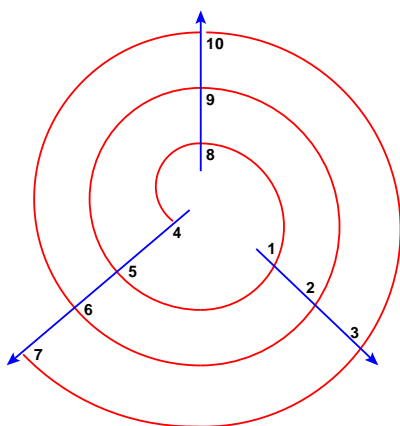


FIGURE 6 – La 10-roubine de multiplicateur 3

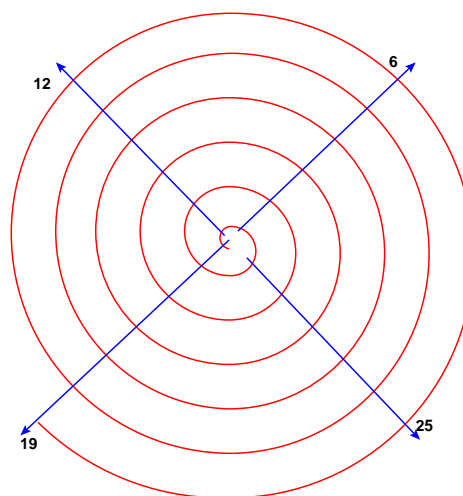


FIGURE 7 – La 25-roubine de multiplicateur 4

## 5 Les spirales

Avec les roubines, et plus précisément, les générateurs congruentsiels, 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 congruentsiel. 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 2 qui permet d'obtenir une permutation spirale pour tout  $n$ . Les *spinines* sont définies dans [Roubaud, 2000] comme des permutations obtenues par effacements à partir de quenines. Nous choisissons alors de dénommer *spirallines* ces nouvelles permutations.

**DÉFINITION 2.** Soient  $n \in \mathbb{N}$  et  $g$  premier avec  $n$ . La  $n$ -spiralline de multiplicateur  $g$ , ou  $n, g$ -spiralline, est la permutation de  $1..n$  dans  $1..n$  vérifiant  $\gamma_{n,g}(m) \equiv 1 - g \cdot m \pmod{n}$ .

**THÉORÈME 3.** Une  $n, g$ -spiralline 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 spirallines 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 spirallines d'ordre  $n$ . La figure 9 est à comparer avec la roubine de mêmes paramètres, figure 7.

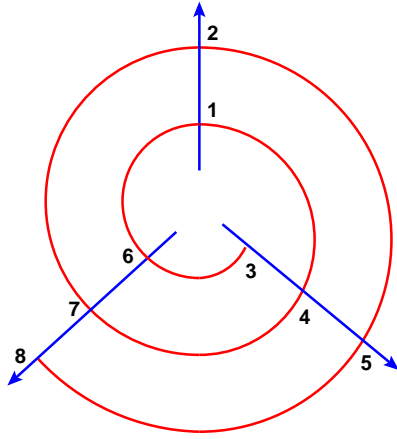


FIGURE 8 – La 8-spiralline de multiplicateur 3

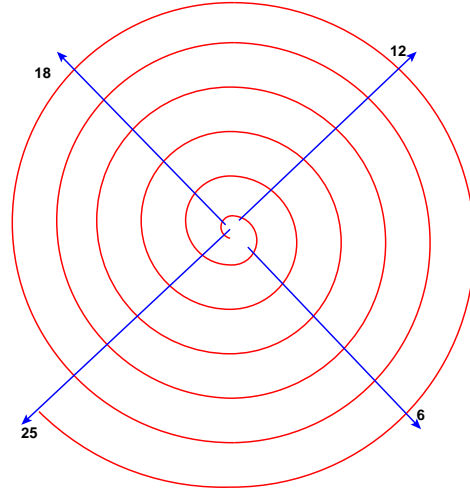


FIGURE 9 – La 25-spiralline de multiplicateur 4

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 spirallines (pour tout  $n$ ), tous les entiers possèdent dorénavant au moins une permutation spirale. Néanmoins, quand  $n$  est sans carré, les roubines impaires et les spirallines nécessitent d'avoir  $n - 1$  rayons d'après le théorème 3. Leur esthétique est donc assez réduite. On parlera alors de **jolie** spiralline 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.

**DÉFINITION 3.** Une permutation spirale est **jolie** si et seulement si chaque rayon comporte au moins 2 entiers.

Il reste tout de même assez peu d'entiers ne possédant pas de jolie spiralline, la table 4 recense ceux inférieurs à 1000.

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 spirallines.

## 6 Toutes les permutations spirales

Grâce à la notion de rayon, nous pouvons encore étendre la notion de permutation spirale à partir de la représentation graphique : toute permutation ayant une représentation spirale avec

|     |     |     |     |     |     |     |     |     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 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 spiruline

des rayons sur lesquels les entiers sont consécutifs, quelque soit l'orientation et la séquence de ces rayons, cf définition 1.

Afin de pouvoir décrire ces permutations, nous définissons une syntaxe des rayons : ceux-ci peuvent être entrants ou sortants comme en section 3 et nous donnons les entiers extrêmes du rayon, les autres étant consécutifs, de l'extérieur de la spirale vers l'intérieur comme explicité table 5.

| Direction         | Signification                              |
|-------------------|--|
| $x \leftarrow y$  | rayon sortant, décroissant de $x$ vers $y$ |
| $x \rightarrow y$ | rayon entrant, croissant de $x$ vers $y$   |

TABLE 5 – Syntaxe des rayons de spirale

Par exemple, la 25-spiraline de multiplicateur 4, figure 9, peut se décrire simplement par  $[25 \leftarrow -196 \leftarrow -112 \leftarrow -718 \leftarrow -13]$  et la 5-dixhuitine, figure 1, par  $[15 \rightarrow 187 \leftarrow -48 \rightarrow 1114 \leftarrow -121 \rightarrow 3]$ .

Le nombre de possibilités est donc exponentiel par rapport à  $n$ . Nous pouvons néanmoins distinguer certaines familles. Par exemple nous parlerons de permutation **ordonnée** si les valeurs maximales de chaque rayon se suivent dans la syntaxe de manière décroissante.

**DÉFINITION 4.** Une permutation spirale est **ordonnée** si et seulement si les entiers maximaux des rayons sont strictement décroissants.

Nous pouvons aussi dire naturellement qu'une permutation est **entrante** (resp. **sortante**) si tous ses rayons sont entrants (resp. sortants).

Avec ce nombre de possibilités décuplé, nous pouvons, enfin, donner deux jolies septines ordonnées, figure 10, celle de gauche étant sortante.

La table 6 donne des jolies permutations ordonnées, à nombre minimal de rayons, pour les premiers des entiers de la table 4, qui en étaient dépourvus.

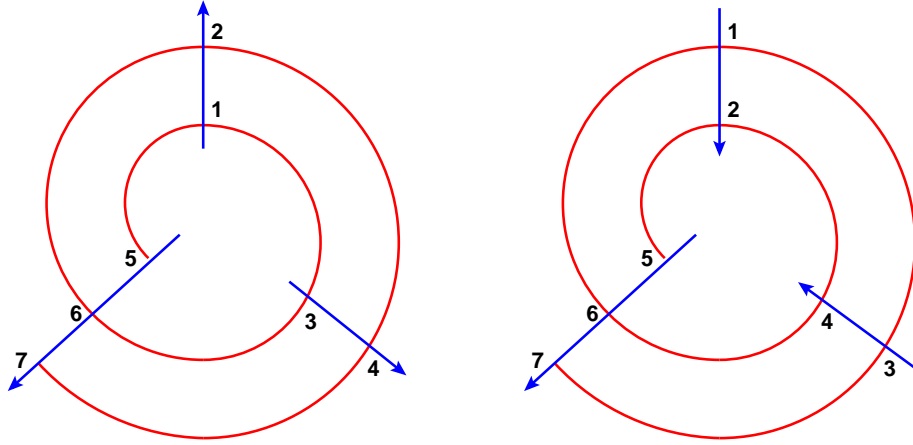


FIGURE 10 – Septines ordonnées

| $n$ | $g$ | Rayons de la permutation  |
|-----|-----|---|
| 7   | 3   | [7<-5 3->4 1->2]  |
| 13  | 4   | [13<-10 7->9 6<-4 3<-1]   |
| 17  | 6   | [15->17 14<-12 9->11 8<-6 3->5 2<-1]                              |
| 19  | 5   | [16->19 12->15 11<-8 7<-4 1->3]                                   |
| 31  | 3   | [31<-21 11->20 1->10]   |
| 34  | 4   | [26->34 25<-17 16<-9 8<-1]  |
| 37  | 10  | [37<-34 30->33 29<-26 25<-22 21<-18 14->17 13<-10 7->9 6<-4 3<-1] |
| 38  | 8   | [38<-34 33<-29 28<-24 23<-19 18<-14 9->13 5->8 1->4]              |
| 43  | 7   | [43<-37 36<-31 30<-25 24<-19 18<-13 7->12 1->6]                   |
| 47  | 6   | [47<-40 39<-32 24->31 23<-16 15<-8 1->7]                          |
| 55  | 4   | [42->55 28->41 14->27 13<-1]                                      |
| 57  | 6   | [48->57 38->47 37<-28 27<-19 18<-10 9<-1]                         |
| 59  | 5   | [59<-48 47<-36 35<-24 23<-12 1->11]                               |
| 61  | 6   | [61<-51 41->50 40<-31 21->30 20<-11 1->10]                        |

TABLE 6 – Quelques jolies permutations spirales ordonnées à nombre minimal de rayons

Par recherche exhaustive, il est en effet possible de déterminer le nombre minimal de rayons pour une jolie permutation spirale ordonnée. La table 7 recense le nombre minimal de rayons pour les jolies permutations spirales inférieures à 500.

Enfin, la table 8 donne le plus petit entier nécessitant au moins  $g \leq 19$  rayons pour obtenir une jolie permutation spirale.

Ces données empiriques nous indiquent qu'au prix d'une orientation quelconque des rayons il semble toujours possible de trouver de jolies permutations spirales.

- CONJECTURES 1.**
- i. Tout entier possède une jolie permutation spirale.*
  - ii. Tout entier possède une jolie permutation spirale ordonnée.*
  - iii. Le rayon minimal d'une jolie permutation spirale ordonnée est en  $O(\log(n))$ .*

## 7 Conclusion

Nous avons approfondi les liens entre les permutations spirales, les battements de cartes et les générateurs congruentiels linéaires. Le lien avec les bases normales optimales mériterait plus d'attention, en particulier en quoi une permutation d'ordre maximal peut induire une matrice à nombre d'éléments non nuls minimal. Les périodes de Gauß [Menezes et al., 1993] sont peut-être une clef.

|    |   |    |    |    |    |    |    |    |   |    |    |    |    |    |    |    |    |    |    |
|----|---|----|----|----|----|----|----|----|---|----|----|----|----|----|----|----|----|----|----|
| -  | - | -  | 2  | 2  | 2  | 3  | 3  | 2  | 2 | 2  | 2  | 4  | 2  | 4  | 7  | 6  | 2  | 5  | 3  |
| 5  | 5 | 2  | 8  | 6  | 2  | 2  | 2  | 2  | 2 | 3  | 3  | 2  | 4  | 2  | 2  | 10 | 8  | 2  | 6  |
| 2  | 3 | 7  | 3  | 6  | 7  | 6  | 13 | 6  | 2 | 2  | 2  | 2  | 4  | 4  | 3  | 6  | 2  | 5  | 2  |
| 6  | 5 | 6  | 10 | 2  | 2  | 6  | 3  | 2  | 7 | 7  | 7  | 5  | 2  | 4  | 7  | 6  | 3  | 4  | 8  |
| 2  | 2 | 2  | 8  | 7  | 2  | 8  | 8  | 2  | 2 | 8  | 5  | 5  | 5  | 2  | 7  | 6  | 2  | 2  | 2  |
| 6  | 4 | 6  | 3  | 2  | 2  | 6  | 6  | 7  | 3 | 5  | 11 | 2  | 5  | 10 | 3  | 7  | 6  | 2  | 8  |
| 8  | 5 | 8  | 7  | 3  | 3  | 4  | 3  | 4  | 2 | 2  | 5  | 6  | 2  | 2  | 6  | 11 | 2  | 4  | 3  |
| 5  | 5 | 6  | 8  | 9  | 2  | 10 | 2  | 6  | 5 | 7  | 3  | 6  | 6  | 2  | 6  | 6  | 2  | 5  | 6  |
| 10 | 2 | 9  | 9  | 6  | 8  | 6  | 9  | 9  | 6 | 8  | 2  | 2  | 2  | 3  | 3  | 8  | 2  | 2  | 2  |
| 6  | 6 | 2  | 10 | 10 | 2  | 6  | 10 | 2  | 8 | 2  | 10 | 6  | 2  | 9  | 2  | 7  | 3  | 4  | 3  |
| 6  | 6 | 6  | 8  | 8  | 8  | 8  | 11 | 2  | 2 | 7  | 5  | 9  | 5  | 8  | 7  | 12 | 3  | 10 | 10 |
| 2  | 3 | 6  | 3  | 6  | 2  | 12 | 6  | 10 | 2 | 2  | 6  | 2  | 4  | 9  | 7  | 8  | 7  | 2  | 7  |
| 7  | 4 | 2  | 7  | 2  | 10 | 11 | 11 | 9  | 9 | 2  | 8  | 5  | 2  | 6  | 10 | 8  | 8  | 10 | 3  |
| 2  | 4 | 11 | 12 | 12 | 8  | 7  | 2  | 7  | 2 | 3  | 6  | 2  | 6  | 12 | 6  | 9  | 2  | 6  | 12 |
| 2  | 3 | 8  | 3  | 6  | 7  | 6  | 13 | 9  | 8 | 10 | 2  | 2  | 4  | 7  | 3  | 12 | 7  | 2  | 6  |
| 6  | 4 | 2  | 10 | 4  | 2  | 7  | 3  | 2  | 5 | 8  | 5  | 6  | 7  | 8  | 2  | 6  | 6  | 6  | 3  |
| 8  | 5 | 2  | 7  | 7  | 2  | 7  | 7  | 2  | 2 | 11 | 10 | 10 | 10 | 7  | 8  | 8  | 2  | 8  | 8  |
| 9  | 7 | 9  | 9  | 8  | 2  | 8  | 2  | 6  | 2 | 8  | 6  | 11 | 2  | 12 | 10 | 11 | 8  | 2  | 12 |
| 6  | 6 | 8  | 12 | 10 | 6  | 4  | 6  | 10 | 7 | 2  | 2  | 10 | 3  | 2  | 9  | 10 | 2  | 4  | 4  |
| 7  | 6 | 7  | 9  | 10 | 2  | 10 | 2  | 6  | 6 | 6  | 6  | 2  | 9  | 9  | 6  | 9  | 2  | 10 | 12 |
| 9  | 9 | 12 | 3  | 8  | 7  | 12 | 7  | 5  | 2 | 2  | 5  | 2  | 2  | 8  | 9  | 9  | 2  | 2  | 2  |
| 8  | 7 | 10 | 10 | 10 | 2  | 10 | 3  | 2  | 5 | 2  | 7  | 6  | 4  | 8  | 7  | 8  | 2  | 8  | 3  |
| 2  | 2 | 2  | 14 | 10 | 8  | 7  | 12 | 9  | 7 | 6  | 5  | 2  | 6  | 3  | 9  | 9  | 8  | 10 | 2  |
| 10 | 3 | 10 | 3  | 8  | 2  | 8  | 7  | 9  | 2 | 8  | 10 | 2  | 8  | 4  | 3  | 12 | 12 | 12 | 11 |
| 6  | 7 | 2  | 9  | 3  | 3  | 16 | 3  | 5  | 2 | 2  | 5  | 7  | 6  | 2  | 10 | 6  | 10 | 10 | 12 |

TABLE 7 – Nombre minimal de rayons pour les 500 premières jolies permutations spirales ordonnées

|     |    |     |     |     |      |     |      |      |      |      |        |
|-----|----|-----|-----|-----|------|-----|------|------|------|------|--------|
| $g$ | 2  | 3   | 4   | 5   | 6    | 7   | 8    | 9    | 10   | 11   | 12     |
| $n$ | 4  | 7   | 13  | 19  | 17   | 16  | 24   | 145  | 37   | 112  | 217    |
| $g$ | 13 | 14  | 15  | 16  | 17   | 18  | 19   | 20   | 21   | 22   | 23     |
| $n$ | 48 | 444 | 535 | 487 | 1731 | 784 | 1552 | 4879 | 4087 | 4880 | >10000 |

TABLE 8 – Première occurrence d'un nombre minimal de rayons

Ensuite nous avons donné une construction polynomiale des permutations spirales dépendant de la construction efficace d'une racine primitive.

Enfin, nous avons étendu le bestiaire de Jacques Roubaud aux roubines et aux spirales et avons proposé une alternative, à représentation spirale, à la méthode des effacements, donnant une permutation spirale à tout entier.

## 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.
- [Dubrois and Dumas, 2006] Dubrois, J. and Dumas, J.-G. (2006). Efficient polynomial time algorithms computing industrial-strength primitive roots. *Information Processing letters*, 97(2) :41–45.
- [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<sup>nd</sup> 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.  $n \equiv 1 \pmod{4}$ ;  $+2$  est primitif et  $-2$  d'ordre exactement  $n$  dans  $\mathbb{Z}/2n+1\mathbb{Z}$
- ii.  $n \equiv 2 \pmod{4}$ ;  $+2$  et  $-2$  sont racines primitives dans  $\mathbb{Z}/2n+1\mathbb{Z}$
- iii.  $n \equiv 3 \pmod{4}$ ;  $-2$  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  $n \equiv 0 \pmod{4}$  ou  $n \equiv 3 \pmod{4}$ .
- ii.  $2$  est d'ordre  $n$  est incompatible avec  $n \equiv 1 \pmod{4}$ .
- iii.  $-2$  est d'ordre  $n$  quand  $n \equiv 1 \pmod{4}$ .
- iv.  $-2$  est d'ordre  $2n$  quand  $n \equiv 2 \pmod{4}$ .
- v.  $-2$  est d'ordre  $2n$  et  $2$  est d'ordre  $n$  quand  $n \equiv 3 \pmod{4}$ .

Le caractère de résiduïté 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  $n \equiv 0 \pmod{4}$  (resp.  $n \equiv 3 \pmod{4}$ ) alors  $2n + 1 \equiv 1 \pmod{8}$  (resp.  $2n + 1 \equiv 7 \pmod{8}$ ) 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  $n \equiv 1 \pmod{4}$  alors  $2n + 1 \equiv 3 \pmod{8}$  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  $2^{4k+2} \equiv (2^{2k+1})^2 \equiv 2$  et donc  $2$  serait un résidu quadratique ce qui est absurde.
- iii. Le point précédent et le théorème 1 montrent que lorsque  $n \equiv 1 \pmod{4}$ ,  $2$  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  $n \equiv 2 \pmod{4}$  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  $n \equiv 3 \pmod{4}$ . 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  $e = 2n$ .

□