Caractérisation des Quenines et leur représentation spirale

Jean-Guillaume Dumas

Caractérisation des Quenines et leur représentation spirale

Jean-Guillaume Dumas *

16 novembre 2007

Résumé

Les nombres de Raymond Queneau sont les entiers n pour lesquels la quenine (permutation spirale envoyant tout nombre pair sur sa moitié et tout nombre impair sur son opposé ajouté à n) est d'ordre maximal n. Nous étudions dans cette note la caractérisation des nombres de Queneau, les précédentes caractérisations étant à notre connaissance incomplètes. Nous proposons en outre une nouvelle représentation graphique, sous forme de spirale, à la fois des quenines à racine primitive différente de 2 et également des spinines, généralisation des quenines par la méthode des effacements de Jacques Roubaud.

Summary

The Raymond Queneau numbers are the integers n for which the quenine (the spiral permutation sending even numbers to their halves and odd numbers to their opposites added to n) is of order n. We study in this note the characterization of Queneau numbers, previous being to our knowledge incomplete. We also propose a new graphical representation, of spiral shape, both of the quenines with primitive root distinct from 2 and also to the spinines, which generalize quenines by Jacques Roubaud's erasing technique.

Mots-clefs : Permutation de Queneau-Daniel ; Quenine ; Spinine ; Spirale ; Racine primitive.

1 L'oulipo, la poésie des troubadours et les Quenines

Arnaut Daniel est un troubadour de la fin du XII^e siècle. Un de ses poèmes célèbres, **ongle et oncle**, figure 1, est une série de six strophes de six vers chacune [Roubaud, 1969]. Chacun des mots à la rime de la première strophe est reproduit dans les strophes suivantes dans un autre ordre. Plus précisément, chaque passage d'une strophe à l'autre est déterminé de la même façon, à l'aide de la spirale suivante :

*Laboratoire J. Kuntzmann, 51, rue des Mathématiques. Université de Grenoble. UMR CNRS 5224, BP 53X, F38041 Grenoble, France, Jean-Guillaume.Dumas@imag.fr .

Sextine

Ce vœu dur qui dans le cœur m'entre,
nul bec ne peut le déchirer, ni ongle
de lausengier, qui médisant perd l'âme ;
et ne l'osant battre à branche ou à verge,
secrètement, là où il n'y a point d'oncle,
j'aurai ma joie en verger ou en chambre.

Quand j'ai souvenir de la chambre
où à mon dam je sais que pas un n'entre,
tant me sont durs plus que frère ni oncle
nul membre n'ai qui ne tremble, ni d'ongle,
plus que ne fait l'enfant devant la verge :
telle est ma peur de l'avoir trop dans l'âme !

Puisse-t-elle de corps, non d'âme,
me recevoir en secret dans sa chambre !
Car plus me blesse au cœur que coup de verge
si qui la sert là où elle est ne rentre !
Toujours serai pour elle chair et ongle
et ne croirai conseil d'ami ni d'oncle.

Et jamais la sur de mon oncle
je n'aimai plus ni tant, de par mon âme
Et si voisin que l'est le doigt de l'ongle,
je voudrais être, à son gré, de sa chambre
plus peut L'Amour qui dans le cœur me rentre
faire de moi qu'un fort de frêle verge.

Car depuis que fleurit la verge
sèche et qu'Adam légua neveux et oncles,
si fine amour, qui dans le cœur me rentre,
ne fut jamais en corps, ni même en âme ;
où qu'elle soit, dehors ou dans sa chambre,
mon cœur y tient comme la chair à l'ongle.

Car ainsi se prend et s'énongle
mon cœur en elle ainsi qu'écorce en verge ;
elle est de joie tour et palais et chambre,
et je ne prise autant parents ni oncle :
au ciel j'aurai deux fois joyeuse l'âme,
si jamais nul, de trop aimer, n'y entre.

Arnaud envoie sa chanson d'ongle et d'oncle
à toi qui tiens son âme sous ta verge,
son Désiré, dont le prix en chambre entre.

Sestina

Lo ferm voler qu'el còr m'intra
no'm pùt ges bècs escoissendre ni ongla
de lausengièr, qui pèrd per mal dir s'arma ;
e car non l'aus batre amb ram ni amb verja,
sivals a frau, lai ont non aurai oncle,
jausirai jòi, en vergièr o dins chambra.

Quand mi soven de la chambra
ont a mon dam sai que nulhs òm non intra,
ans me son tuch plus que fraire ni oncle,
non ai membre no'm fremisca, neis l'ongla,
aissì com fai l'énfans denant la verja :
tal paor ai no'l sia tròp de l'arma.

Del còr li fos, non de l'arma,
e consentis m'a celat dins sa chambra !
Que plus mi nafra'l còr que còps de verja
car lo sieus sèrvs lai ont ilh es non intra ;
tots temps serai amb lièis com charns et ongla,
e non creirai chastic d'amic ni d'oncle.

Anc la seror de mon oncle
non amèi plus ni tant, per aquesta'arma !
Qu'aitant vesins com es lo dets de l'ongla,
s'a lièis plagués, vòlgra èsser de sa chambra ;
de mi pòt far l'amors qu'ins el còr m'intra
mièlhs a son vòl qu'òm fòrts de frévol verja.

Puèis florit la secha verja
ni d'En Adam mògron nebot ni oncle,
tant fina amors com cela qu'el còr m'intra
non cug fos anc en còrs, ni eis en arma ;
ont qu'ilh estei, fòrs en plaça o dins chambra,
mos còrs no's part de lièis tant com ten l'ongla.

Qu'aissi s'enpren e s'enongla
mons còrs en lièis com l'escòrça en la verja ;
qu'ilh m'es de jòi tors e palatz e chambra,
e non am tant fraire, parent ni oncle :
qu'en paradis n'aurà doble jòi m'arma,
si ja nulhs òm per ben amar lai intra.

Arnauts tramet sa chançon d'ongla e d'oncle,
a grat de lièis que de sa verja à l'arma,
son Desirat, cui prètz en chambra intra.

FIG. 1 – Ongle et oncle, Arnaut Daniel, XII^{e} siècle

	§1		σ_6 §2	§3	§4	§5	§6
$\mathcal{O}_6(1)$	1	$\rightarrow$	6	3	5	4	2
	2	$\rightarrow$	1	6	3	5	4
	3	$\rightarrow$	5	4	2	1	6
	4	$\rightarrow$	2	1	6	3	5
	5	$\rightarrow$	4	2	1	6	3
	6	$\rightarrow$	3	5	4	2	1

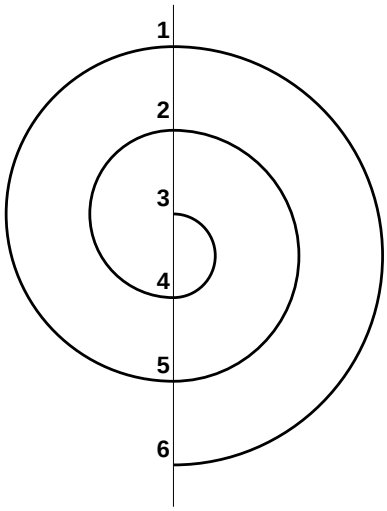

FIG. 2 – Permutation spirale de la sextine

En effet, si l'on inscrit de haut en bas les rimes d'une strophe, dans la strophe suivante, ces rimes se retrouvent dans l'ordre donné lorsque l'on suit les méandres de la spirale : en partant du bas, en 6, on tourne pour rencontrer successivement 1, 5, 2, 4, 3 qui forment bien les rimes de la deuxième strophe. Ce type de permutation sur 6 vers est appelé une sextine et a été généralisé à n vers par Raymond Queneau.

DÉFINITIONS 1. *[Bringer, 1969]*

- *Une* **permutation spirale** *est une permutation σ_n de l'ensemble $\{1, 2, \ldots, n\}$ vérifiant la condition suivante :*

$$\begin{aligned} \sigma_n(2p) &= p \\ \sigma_n(2p+1) &= n-p \end{aligned}$$

- *Le sous-groupe cyclique G_n, engendré par σ_n est le groupe de Queneau-Daniel.*
- *Les entiers n tels que G_n soit de cardinal n sont dits* **admissibles**.
- *Une permutation spirale avec n admissible est appelée une* **quenine**, *ou encore une n^{ine}.*

Autrement dit, n est admissible si et seulement si les **orbites poétiques** de chacune des rimes sont d'**ordre spiralique** n, i.e. chaque rime se trouve une seule fois à un endroit donné de la strophe dans l'ensemble du poème. Arnaut Daniel a exhibé une quenine de cardinal 6, mais toutes les quenines ne sont pas possibles : par exemple, il n'y a pas de quenine de cardinal 4, puisque, par exemple, l'orbite de 3 est le singleton $\{3\}$ [Roubaud, 2000]. L'Oulipo, et plus particulièrement Jacques Roubaud, s'est alors intéressé à la quête des quenines, à l'aide des corps finis.

En effet, considérons la permutation δ_n, inverse de σ_n. Celle-ci peut être définie comme suit :

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

Démonstration. Soit x tel que $2x \leq n$ alors $\sigma_n \circ \delta_n(x) = \sigma_n(2x) = x$. Pour x tel que $2x > n$ alors $\sigma_n \circ \delta_n(x) = \sigma_n(2(n-x)+1) = n-(n-x) = x$. Donc $\sigma_n \circ \delta_n = Id$ et σ_n étant bijective, δ_n est son inverse. □

Il est clair que les cardinaux des sous-groupes cycliques engendrés par δ_n ou σ_n sont identiques. Il revient donc au même d'étudier l'un ou l'autre des sous-groupes. 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 $\delta_n(x) \equiv (-1)^e 2x[2n+1]$. À partir de là Monique Bringer a montré un certain nombre de résultats dont les suivants :

THÉORÈME 1. *[Bringer, 1969]*
- *Si n est admissible alors $2n+1$ est premier.*
- *$n = 4p$ n'est pas admissible.*
- *$n = 2^p - 1$ n'est pas admissible.*
- *Si n et $2n+1$ sont premiers, n est admissible.*
- *Si $n = 2p$ et que p et $4p+1 = 2n+1$ sont premiers, n est admissible.*

Démonstration. Reprenons seulement sa preuve que $2n+1$ est forcément premier. Sinon, il existe q un diviseur de $2n+1$ avec $q > 1$. Dans ce cas, pour tout m de l'orbite de q, on a $m \equiv (-1)^e 2^k q$. Ce qui implique forcément que q divise m puisqu'il divise à la fois $2n+1$ et $(-1)^e 2^k q$. Donc l'orbite de q ne contient que des diviseurs de q. Or, $1, \ldots, q-1$ ne divisent pas q donc l'orbite de q ne peut être complète. Par la suite $2n+1$ ne peut être admissible. □

Or, il est possible de complètement caractériser les quenines. Ceci peut être fait avec un peu de théorie des corps finis.

2 Corps finis

Dans cette section nous rappelons brièvement les propriétés classiques des corps finis en développant particulièrement l'étude des générateurs du groupe des inversibles d'un corps fini, les racines primitives. Nous prenons le parti de donner plusieurs preuves, même classiques, afin de regrouper dans cette note les éléments essentiels à la fabrication des quenines. Plus de détails sont à trouver bien sûr dans les ouvrages de référence comme par exemple [Lidl and Niederreiter, 1994, Burton, 1998, Demazure, 1997, Dumas et al., 2007].

DÉFINITION 1. *Le corps des nombres rationnels $\mathbb{Q}$ et les corps $\mathbb{Z}$, pour p premier, sont appelés* **corps premiers**. *Les corps finis sont appelés* **corps de Galois**. *Ils sont notés $\mathbb{F}_q$ ou $\mathtt{GF}(q)$, avec q le cardinal du corps.*

PROPOSITION 1. *Soit $(K,+,\times)$ un corps fini de cardinal $q>0$. On note*

$$n.1_K = \underbrace{1_K + 1_K + \ldots + 1_K}_{n \textit{ fois}}.$$

La **caractéristique** *de K est le nombre premier p tel que $p.1_K = 0$.*

Démonstration. Définissons $\Psi : \mathbb{Z} \to K$ par :

$$\text{Pour tout } n \in \mathbb{Z},\ \Psi(n) = \underbrace{1_K + 1_K + \ldots + 1_K}_{n \text{ fois}} = n.1_K,$$

On a tout d'abord $\Psi(0) = 0_K, \Psi(1) = 1_K, \Psi(n_1+n_2) = \Psi(n_1)+\Psi(n_2)$. Ensuite, comme la multiplication d'éléments de K est associative, on obtient

$$\begin{aligned}\Psi(n_1) \times \Psi(n_2) &= \underbrace{(1_K + 1_K + \ldots + 1_K)}_{n_1} \times \underbrace{(1_K + 1_K + \ldots + 1_K)}_{n_2} \\ &= \underbrace{(1_K \times 1_K + \ldots + 1_K \times 1_K)}_{n_1 n_2} = \underbrace{(1_K + \ldots + 1_K)}_{n_1 n_2} = \Psi(n_1 n_2)\end{aligned}$$

et donc Ψ est un homomorphisme d'anneau. Comme K est fini et $\mathbb{Z}$ infini, Ψ est non-injectif, en conséquence, il existe $n \neq 0$ tel que $\Psi(n) = 0_K$ (si $\Psi(j) = \Psi(i)$ pour $j \neq i$ alors $n = |j - i|$ convient).

Si n n'est pas premier, soit $n = n_1 n_2$. On a $\Psi(n_1) \times \Psi(n_2) = 0_K$ donc $\Psi(n_1) = 0_K$ ou $\Psi(n_2) = 0_K$ (K est un corps donc ses éléments non nuls sont inversibles). Donc il existe p premier tel que $\Psi(p) = 0_K$.

Pour l'unicité de p : si p_1 et p_2 sont premiers et $\Psi(p_1) = \Psi(p_2) = 0_K$. alors, d'après Bézout, il existe a, b tels que $ap_1 + bp_2 = 1$ d'où $\Psi(1) = 0_K$, ce qui est absurde. □

PROPOSITION 2. *Soit $(K,+,\times)$ un corps fini de cardinal $q>0$ et $a \neq 0_K \in K$. On note*

$$a^n = \underbrace{a \times a \times \ldots \times a}_{n \textit{ fois}}.$$

*L'***ordre** *d'un inversible a est le plus petit entier strictement positif o tel que $a^o = 1_K$.*

Démonstration. Soit $O_a = \{a, a^2, a^3, \ldots\}$ l'**orbite** de a. Comme K est fini, O_a aussi et donc il existe i et j avec $i > j$ tels que $a^i = a^j$. comme a est inversible, on obtient $a^{i-j} = 1_K$, avec $i - j > 0$. L'ensemble des entiers positifs vérifiant $a^o = 1_K$ est donc non vide, il contient donc un plus petit élément. □

On a également les propriétés classiques suivantes :

PROPRIÉTÉS 1.

i.) Si un corps W est un sous-corps d'un corps V, alors V a une structure d'espace vectoriel sur le corps W (la multiplication d'un élément de F par un élément de V est considérée comme le produit d'un scalaire par un vecteur).

ii.) Si la caractéristique d'un corps fini est non nulle, le cardinal du corps est une puissance de la caractéristique.

iii.) Tous les corps finis de même cardinal sont isomorphes (deux corps sont isomorphes s'ils le sont en tant qu'anneaux).

iv.) Le cardinal de tout sous-corps d'un corps fini est un diviseur du cardinal du corps.

v.) L'ordre de tout inversible d'un corps fini est un diviseur du cardinal du groupe des inversibles du corps.

vi.) Le groupe des inversibles, $\mathbb{F}^*$, d'un corps fini $\mathbb{F} = \mathtt{GF}(q)$ est cyclique de cardinal $q-1$.

Démonstration. Nous ne donnons ici que quelques unes des preuves, classiques.
de ii.) Soit V un corps fini. Le cardinal de V est noté $|V|$. Alors V est de caractéristique $p \neq 0$ et p est un nombre premier. Le corps V est un espace vectoriel sur son sous-corps premier $F = \{k \cdot 1 \ : \ k = 1, \ldots, p\}$ et cet espace vectoriel est de dimension finie (sinon V ne serait pas fini). Si l'on prend $d = \dim_F V$, alors $|V| = p^d$.
de iii.) si d=1
On suppose $|V| = p$ (c'est à dire $d = 1$). L'application $\phi \ : \ \mathbb{F}_p \longrightarrow V$ qui à tout $k \in \mathbb{F}_p$ associe $\phi(k) = k \cdot 1$ est un isomorphisme.
de iii.) en général
Soit W un corps fini de cardinal p^d. Le sous-corps premier de W ainsi que celui de V sont tous les deux isomorphes à $\mathbb{F}_p$ (d'après l'énoncé **d=1** précédent) donc V et W s'identifient chacun à un $\mathbb{F}_p$-espace vectoriel. Et puisque les $\mathbb{F}_p$-espaces vectoriels V et W ont la même dimension d, ils sont isomorphes.
v.) Pour a un inversible, on divise $q-1$ par son ordre o pour obtenir $q-1 = bo+r$. Alors $a^r = a^{q-1} \left(a^o\right)^{-b} = 1$. Or o est le plus petit entier strictement positif vérifiant cela donc $r = 0$.
vi.) Il s'agit de démontrer l'existence d'un générateur. Nous avons tout d'abord besoin du lemme suivant :

LEMME 1. *Soient x et y d'ordres m et n. xy est d'ordre $ppcm(m,n)$.*

Preuve du lemme. Soient $d = pgcd(m,n)$ et $m = dm'$, $n = dn'$. Alors x^d ety^d sont d'ordres m' et n' premiers entre eux. Il s'en suit que $(x^d y^d)^{m'n'} = 1_{\mathbb{F}_q}$. Réciproquement si $(x^d y^d)^r = 1$, alors $(x^d y^d)^{rm'} = 1$ et donc $(y^d)^{rm'} = 1$. Ce qui prouve que n', l'ordre de y^d, divise rm', et donc r puisque n' et m' sont premiers entre eux. De même m' divise r, et l'on conclut que l'ordre de $x^d y^d$ est bien $m'n'$ et ainsi que l'ordre de xy est $dm'n' = ppcm(m,n)$. □

À partir de là, nous posons $\omega = ppcm($ ordres d'éléments de $\mathbb{F}_q)$. Donc ω est le plus petit entier tel que $x^\omega = 1_{\mathbb{F}_q}$ pour tous les éléments du corps. Par suite ω doit diviser $q-1$ puisque par Lagrange, $x^{q-1} = 1_{\mathbb{F}_q}$ pour tout inversible. Ensuite, puisque le polynôme $x^\omega - 1$ ne peut avoir qu'au plus ω racines dans un corps et que tous les inversibles du corps en sont racines, il faut nécessairement que $\omega = q-1$. Enfin, le lemme nous permet de construire un élément d'ordre ω. □

3 Caractérisation des quenines

Nous rappelons qu'un générateur du groupe des inversibles d'un corps fini est appelé une **racine primitive de l'unité**. En effet c'est une racine $q-1$-ième de 1 et la primitivité vient du fait qu'elle n'est pas une racine d'ordre inférieur.

Nous avons vu que Monique Bringer a donné une condition suffisante et les cas particuliers du théorème 1 ; Jacques Roubaud donne une caractérisation dans [Roubaud, 2000, 2.4.II] qui semble incorrecte : « Une condition nécessaire et suffisante pour que n soit admissible est qu'il soit d'ordre n ou $2n$ dans le groupe multiplicatif des entiers modulo 2. »

Dans cette caractérisation, le cas où n est pair n'est pas considéré : un contre exemple simple est celui de l'octine : 2 est d'ordre 8 modulo 17, mais malheureusement l'orbite de 2 n'est que d'ordre spiralique 4, ce qui rend l'octine impossible.

Nous donnons donc ici une caractérisation complète :

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 $\mathbb{Z}/2n+1\mathbb{Z}$.*

Démonstration. Tout d'abord prouvons la condition nécessaire. Comme l'ordre de 2 divise $2n$, le cardinal des inversibles de $\mathbb{Z}/2n+1\mathbb{Z}$, les seuls ordres possibles, différents de n et $2n$, sont strictement inférieurs à n. Supposons que 2 est d'ordre $j < n$. Alors nous avons $\delta_n^j(2) \equiv \pm 2^j 2 \equiv \pm 2$. Nous avons donc deux cas :

1. Si $\delta_n^j(2) = 2$, alors l'orbite de 2 ne contient que $j < n$ éléments, ce qui n'est pas suffisant car n est supposé admissible.
2. Dans l'autre cas, $\delta_n^j(2) \equiv -2$. Alors cela veut dire qu'il existe $h = \delta_n^{j-1}(2)$, donc vérifiant $0 \leq h \leq n$ et tel que $\delta_n(h) \equiv -2$. En prenant maintenant la définition de δ_n, nous avons encore deux cas, suivant h :
   (a) si $\delta_n(h) = 2h$ alors $2h \equiv -2$, ce qui veut dire que $2h+2 = k(2n+1)$. Or $h \leq n$, donc $k = 1$, ce qui est absurde, car $2h+2$ serait alors impair.
   (b) Donc l'autre possibilité est que $\delta_n(h) = 2n+1-2h$. Ainsi, toujours avec la majoration de h, on obtient $2n+1-2h = 2n+1-2$ et donc $h = 1$ et $2h > n$, c'est-à-dire que $n \leq 1$.

   Donc le seul cas pour lequel l'ordre de 2 peut être strictement inférieur à n est $n = 1$. Or 2 est d'ordre 2 modulo 3.

Donc si n est admissible, alors 2 est d'ordre n ou $2n$ modulo $2n+1$.

Il ne nous reste plus qu'à exclure le cas où $n = 2p$ est pair et 2 est d'ordre n modulo $2n+1$. En effet, dans ce cas $2^p \equiv -1\ [2n+1]$. Il s'en suit que $\delta_n^p(2) \equiv (-1)^k 2^p 2 \equiv \pm 2$. Or, si $\delta_n^p(2) \equiv -2$, cela veut dire, encore une fois, qu'il existe h tel que $\delta_n(h) \equiv -2$, nous avons vu qu'alors $n \leq 1$ ce qui donne $n = 0$, puisque n est pair. Il s'en suit de nouveau que la seule possibilité est $\delta_n^p(2) \equiv 2$. Mais alors n n'est pas admissible puisque l'orbite de 2 par δ_n ne contient qu'au

plus $p = \frac{n}{2} < n$ éléments distincts.

Nous prouvons ensuite la condition suffisante. Prenons ω le cardinal de la plus petite orbite des éléments de $\{1, \ldots, n\}$ par δ_n et supposons que l'élément u soit d'ordre ω. Dans ce cas, le fait qu'il existe k tel que $\delta_n^\omega(u) \equiv u \equiv (-1)^k 2^\omega u$. implique donc que $(-1)^k 2^\omega \equiv 1$, car u est inversible.

1. Considérons tout d'abord que 2 est une racine primitive, alors $2^n \equiv -1\ [2n+1]$, puisque 2^n ne peut pas valoir 1 et que la seule autre racine carrée de 1 est -1. Donc $(2^n)^k 2^\omega \equiv 1$. Or l'ordre de 2 est $2n$ ce qui implique que $2n$ divise $nk + \omega$, donc que ω est un multiple de n, et toutes les orbites sont d'ordre n.
2. Enfin, si 2 est d'ordre n. Alors on a de même $(-1)^k 2^\omega \equiv 1$. Dans ce cas, on élève au carré et $(2^\omega)^2 \equiv 1$, donc 2ω est un multiple de n, l'ordre de 2. Or n est impair, donc par le lemme de Gauß, ω est, dans ce cas également, un multiple de n.

□

Ainsi, nous pouvons décider facilement si une quenine donnée existe ou non. La table 1 donne les 178 premières quenines[1].

1	2	3	5	6	9	11	14	18	23	26	29	30
33	35	39	41	50	51	53	65	69	74	81	83	86
89	90	95	98	99	105	113	119	131	134	135	146	155
158	173	174	179	183	186	189	191	194	209	210	221	230
231	233	239	243	245	251	254	261	270	273	278	281	293
299	303	306	309	323	326	329	330	338	350	354	359	371
375	378	386	393	398	410	411	413	414	419	426	429	431
438	441	443	453	470	473	483	491	495	509	515	519	530
531	543	545	554	558	561	575	585	593	606	611	614	615
618	629	638	639	641	645	650	651	653	659	683	686	690
713	719	723	725	726	741	743	746	749	755	761	765	771
774	779	783	785	791	803	809	810	818	831	833	834	846
866	870	873	879	891	893	911	923	930	933	935	938	939
950	953	965	974	975	986	989	993	998				

TABLE 1 – Les quenines inférieures à 1000

4 Généralisations des quenines

Notons que Jacques Roubaud généralise les quenines aux k-quenines, permutations pour lesquelles la multiplication par 2 est remplacée par une multi-

[1] Dans [Roubaud, 2000], Jacques Roubaud indique que 141 est une quenine, ceci est inexact [Esposito-Farèse, 2000] : en particulier, 2 est d'ordre seulement $94 = 2 * 47 < 141 = 3 * 47$ modulo 283.

plication par k, considérons $\delta_{3,n}(x)$:

$$\delta_{3,n}(x) = \begin{cases} 3x & \text{si } 3x \leq n \\ 2n+1-3x & \text{si } n < 3x \leq 2n \\ 3x-(2n+1) & \text{sinon} \end{cases}$$

Notons que $2n+1$ étant premier, $3x$ ne peut pas être égal à $2n+1$. Cette généralisation donne par exemple directement l'octine, ou 3-quenine : $1 \quad \rightarrow \quad 6 \;\; 2 \;\; 5 \;\; 4 \;\; 7 \;\; 8 \;\; 3$.

La table 2 donne les entiers dont 3 est une racine primitive de $2n+1$, premier, qui ne sont pas des 2-quenines.

8	15	21	44	56	63	68	111	116	125$^\diamond$	128	140	141
165	176	200	224	260	284	285	296	308	315	320	345	369
404	405	428	440	455$^\diamond$	464	476	485$^\diamond$	488	506	524	548	551$^\diamond$
581$^\diamond$	596	608	663	680	704	711	716	729	740	776	789	800
806	813	848	849	854	860	861	905$^\diamond$	915	944	956	999	

TABLE 2 – Les 3-quenines inférieures à 1000 qui ne sont pas des 2-quenines. $^\diamond$ indique que 3 est d'ordre n dans $\mathbb{Z}/2n+1\mathbb{Z}$.

La représentation en spirale n'est par contre plus valable, il faut l'adapter à la racine primitive 3, i.e. aux trois cas possibles dans la définition de σ ou δ. L'idée est de considérer 3 "rayons" comme sur la figure 3.

Comme il est possible d'utiliser n'importe quelle racine primitive, il faut donc généraliser cette représentation : la spirale un nombre de rayons exactement égal à la racine primitive utilisée. Par exemple, la 2-dixhuitine existe, mais on peut préférer la 5-dixhuitine qui est donnée sur la figure 4.

Ainsi, tous les entiers n dont $2n+1$ est premier permettent d'avoir une permutation spirale généralisée. Il suffit de savoir fabriquer des racines primitives. En particulier, la plus petite racine primitive est intéressante puisqu'elle permet d'avoir la représentation spirale la plus "simple" en ce sens qu'elle présente le moins de rayons possibles.

DÉFINITION 2. *La* **plus petite racine primitive** *de m est notée $\chi(m)$.*

5 Racines primitives

Nous commençoons par prouver que nous avons un certain choix, puisque les racines primitives sont nombreuses.

PROPOSITION 3. *Il y a $\varphi(q-1)$ racines primitives dans $\mathtt{GF}(q)$.*

Démonstration. La preuve est classique. Soit g un générateur et soit k premier avec $q-1$, alors g^k est un générateur. En effet, si $(g^k)^x = 1$ alors $ku+(q-1)v = 1$ implique que $g^{kxu} = g^{x+vx(q-1)} = g^x = 1$ et donc $x \geq (q-1)$. □

Ensuite, nous donnons la façopn classique de savoir si un nombre donné est une racine primitive ou non. Malheureusement ce test n'est pas polynomial car il nécessite de factoriser $\varphi(n)$. Il suffit ensuite de tester si l'ordre de l'élément est bien $\varphi(m)$:

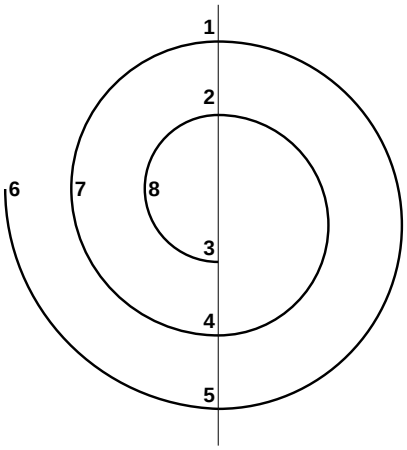

FIG. 3 – La 3-octine

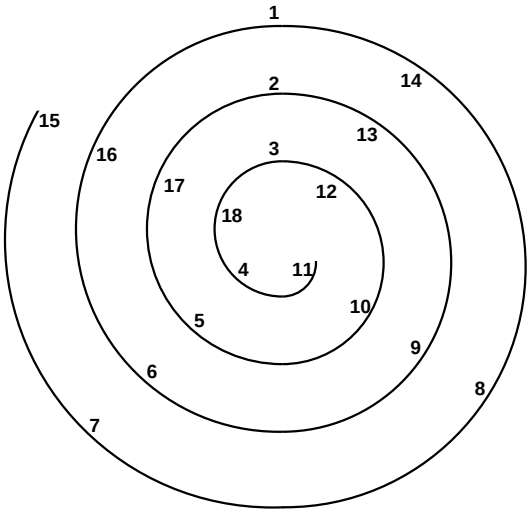

FIG. 4 – La 5-dixhuitine

ALGORITHME 1 *Test-Racine-Primitive*

Entrée Un entier $m > 0$.

Entrée Un entier $a > 0$.

Sortie Oui, si a est une racine primitive de m ; Non dans le cas contraire.

1: **Si** a et m ne sont pas premiers entre eux **Alors**
2: Renvoyer "Non".
3: **Fin Si**
4: $\varphi_m = \varphi(m)$ {Factorisation de m et calcul par les propriétés multiplicatives de φ}
5: **Pour tout** p, premier et divisant φ_m, **Faire** {Factorisation de $\varphi(m)$}
6: **Si** $a^{\frac{\varphi_m}{p}} \equiv 1[m]$ **Alors**
7: Renvoyer "Non".
8: **Fin Si**{Calcul récursif par carrés}
9: **Fin Pour**
10: Renvoyer "Oui".

THÉORÈME 3. *L'algorithme* Test-Racine-Primitive *est correct.*

Démonstration. La preuve est classique, par exemple : soit un entier a, d'ordre k modulo m. Alors $a^h \equiv 1[m]$ si et seulement si $k|h$. On en déduit que si l'ordre de a est plus petit que $\varphi(m)$, comme il doit diviser $\varphi(m)$, nécessairement l'une des valeurs $\frac{\varphi_m}{p}$ sera un multiple de l'ordre de a. Dans le cas contraire, la seule valeur possible pour l'ordre de a est $\varphi(m)$. □

Une première méthode de calcul est alors d'essayer un à un tous les entiers plus petits que m, qui ne soient ni 1, ni -1, ni une puissance sur les entiers, et de trouver ainsi la plus petite racine primitive de m. De nombreux résultats théoriques existent [Murata, 1991, Elliott and Murata, 1997] prouvant qu'en général, il ne faut pas trop d'essais pour la trouver, de l'ordre de

$$\chi(m) = \mathcal{O}\left(r^4(\log(r)+1)^4 \log^2(m)\right)$$

avec r le nombre de facteurs premiers distincts de m [Shoup, 1992]. En pratique, $\chi(m)$ semble être encore plus petit ; d'après Tomás Oliveira e Silva [Oliveira e Silva, 2000], il apparaît qu'environ 80% des nombres premiers inférieurs à 8910000000000 ont une racine primitive plus petite que 6 et, même, 306841261647 des plus petites racines primitives, sur ces 309582581120 premiers nombres premiers, sont plus petites que 23. Ainsi, dans plus de 99% de ces cas, il suffira de 18 tests pour découvrir une racine primitive d'un nombre premier.

Une autre méthode est de tirer aléatoirement des entiers plus petits que m et de tester si ceux-ci sont une racine primitive ou non. Étant donné qu'il y a $\varphi(p-1)$ racines primitives dans $\mathbb{Z}$ pour p premier, la probabilité d'en trouver une est de $\frac{\varphi(p-1)}{p-1}$ et donc l'espérance du nombre de tirages pour tomber sur une racine primitive est de $\frac{p-1}{\varphi(p-1)}$. Ce qui nous donne une meilleure chance que la force brute puisque Rosser et Schoenfeld [Rosser and Schoenfeld, 1962, Théorème 15] ont montré l'inégalité suivante où C est la constante d'Euler, $C \approx 0.5772156649\ldots$:

$$\frac{m}{\varphi(m)} < e^C \log(\log(m)) + \frac{5}{2\log(\log(m))}, \forall m \geq 3, m \neq 223092870 \qquad (1)$$

En outre, comme $223092871 = 317 \times 703763$ n'est pas premier, nous pouvons utiliser cette inégalité pour toutes les racines primitives de nombres premiers. Il est de plus conjecturé que $e^C \log(\log(m)) < \frac{m}{\varphi(m)}$ pour un nombre infini de m, cette borne semble donc très bonne. Ainsi, pour $7 \leq m \leq 8910000000000$, elle donne une valeur maximale d'environ 6.78330. En pratique c'est encore mieux, puisqu'il y a seulement 36 nombres premiers inférieurs à 10000000000 avec $\frac{p-1}{\varphi(p-1)} > 6.0$.

6 La quête des spinines

En particulier, la table 3 donne la liste des p-quenines inférieures à 1000 avec leur plus petite racine primitive.

1*(2)	2 (2)	3 (2)	5 (2)	6 (2)	8 (3)	9 (2)	11 (2)	14 (2)	15 (3)
18 (2)	20 (6)	21 (3)	23 (2)	26 (2)	29 (2)	30 (2)	33 (2)	35*(2)	36 (5)
39 (2)	41*(2)	44*(3)	48 (5)	50 (2)	51 (2)	53*(2)	54 (6)	56 (3)	63 (3)
65 (2)	68 (3)	69 (2)	74 (2)	75 (5)	78 (5)	81 (2)	83 (2)	86 (2)	89 (2)
90 (2)	95*(2)	96 (5)	98*(2)	99 (2)	105 (2)	111 (3)	113*(2)	114 (6)	116 (3)
119 (2)	120 (7)	125 (3)	128 (3)	131 (2)	134 (2)	135 (2)	138 (5)	140 (3)	141 (3)
146*(2)	153 (5)	155*(2)	156 (10)	158 (2)	165 (3)	168 (10)	173*(2)	174 (2)	176 (3)
179*(2)	183 (2)	186 (2)	189 (2)	191 (2)	194 (2)	198 (5)	200*(3)	204 (21)	209 (2)
210 (2)	215*(5)	216 (5)	219 (5)	221*(2)	224 (3)	228 (13)	230 (2)	231 (2)	233*(2)
239*(2)	243 (2)	245 (2)	249 (5)	251 (2)	254 (2)	260 (3)	261 (2)	270 (2)	273 (2)
278*(2)	281*(2)	284*(3)	285 (3)	288 (5)	293*(2)	296 (3)	299*(2)	300 (7)	303 (2)
306 (2)	308 (3)	309 (2)	315 (3)	320 (3)	321 (7)	323 (2)	326*(2)	329 (2)	330 (2)
336 (5)	338*(2)	341*(5)	345 (3)	350 (2)	354 (2)	359*(2)	363 (5)	366 (6)	369 (3)
371 (2)	375 (2)	378 (2)	380*(6)	384 (11)	386 (2)	393 (2)	398 (2)	404 (3)	405 (3)
410 (2)	411 (2)	413*(2)	414 (2)	419*(2)	426 (2)	428 (3)	429 (2)	431 (2)	438 (2)
440*(3)	441 (2)	443 (2)	453 (2)	455*(3)	459 (5)	464*(3)	468 (5)	470 (2)	473*(2)
476 (3)	483 (2)	485 (3)	488 (3)	491 (2)	495 (2)	498 (7)	504 (11)	506 (3)	509 (2)
510 (10)	515 (2)	516 (5)	519 (2)	524*(3)	525 (5)	530 (2)	531 (2)	534 (6)	543 (2)
545 (2)	546 (5)	548 (3)	551 (3)	554 (2)	558 (2)	561 (2)	564 (11)	575*(2)	576 (5)
581*(3)	585 (2)	590 (7)	593*(2)	596 (3)	600 (11)	606 (2)	608 (3)	611 (2)	614 (2)
615 (2)	618 (2)	624 (7)	629 (2)	638*(2)	639 (2)	641*(2)	644 (6)	645 (2)	648 (10)
650 (2)	651 (2)	653*(2)	659*(2)	660 (13)	663 (3)	680*(3)	683 (2)	686*(2)	690 (2)
699 (5)	704 (3)	711 (3)	713*(2)	714 (6)	716 (3)	719*(2)	723 (2)	725 (2)	726 (2)
729 (3)	735 (5)	740*(3)	741 (2)	743 (2)	744 (14)	746 (2)	749 (2)	755*(2)	761*(2)
765 (2)	771 (2)	774 (2)	776 (3)	779*(2)	783 (2)	785 (2)	789 (3)	791 (2)	798 (11)
800 (3)	803 (2)	804 (7)	806 (3)	809 (2)	810 (2)	813 (3)	818 (2)	828 (11)	831 (2)
833*(2)	834 (2)	846 (2)	848 (3)	849 (3)	854 (3)	860 (3)	861 (3)	866*(2)	870 (2)
873 (2)	876 (7)	879 (2)	888 (5)	891 (2)	893*(2)	894 (6)	900 (11)	905 (3)	911 (2)
915 (3)	923 (2)	930 (2)	933 (2)	935*(2)	936 (10)	938*(2)	939 (2)	944 (3)	950 (2)
953*(2)	956 (3)	965 (2)	966 (5)	974 (2)	975 (2)	986*(2)	989 (2)	993 (2)	996 (5)
998*(2)	999 (3)								

TABLE 3 – Les p-quenines inférieures à 1000 avec p, minimal, entre parenthèses. $*$ indique que p est d'ordre seulement n dans $\mathbb{Z}/2n+1\mathbb{Z}$.

Il à noter qu'il est possible de fabriquer des racines primitives, au moins de manière probabiliste, avec un algorithme polynomial (donc ne nécessitant pas de factorisation de φ ni d'exploration exhaustive de l'ordre) [Dubrois and Dumas, 2006]. Il semble donc possible de fabriquer de manière effective des quenines pour tout n tel que $2n+1$ est premier.

Dans [Roubaud, 2000], Jacques Roubaud se désole néanmoins que seuls les entiers n tels que $2n+1$ soit premier possèdent une permutation spirale. Il propose alors une généralisation à tous les nombres en procédant par effacement ce qui donne l'algorithme général 2 de fabrication de pseudo-quenines ou spinines.

DÉFINITION 3. *La* n**-spinine**, *ou* n*-ine puisqu'il n'y a pas d'ambiguïté est la permutattion obtenue par effacements sur la* $\chi(m)$*-*m*-ine spirale avec* m *le plus petit entier supérieur à* n *tel que* $2m+1$ *est premier.*

Ainsi, on peut fabriquer pour tout n des permutations (ça on le savait déjà !)

ALGORITHME 2 Spinine[Roubaud, 2000]

Entrée Un entier $n > 0$ *quelconque*.

Sortie La spinine d'ordre n.

1: Trouver le plus petit $m \geq n$ tel que $2m + 1$ soit premier.

2: Fabriquer la $\chi(m)$-m-ine, ou si m est trop grand une m-ine quelconque en fabriquant une racine primitive industrielle.

3: Fabriquer l'orbite spiralique de 1 de la m-ine. Cela permet de vérifier (mais de manière non polynomiale en la taille de n) si la racine obtenue ci-dessus est bien primitive.

4: Dans cette orbite spiralique de 1, **effacer** tous les entiers supérieurs à n.

5: L'orbite ainsi obtenue est périodique de période n.

qui proviennent d'une permutation spirale. Afin de différencier les permutations, nous notons la 7-spinine (ou plus simplement la septine), obtenue par effacement de 8 dans la 3-octine, comme $3;8$-septine. Par opposition, la permutation qui serait obtenue par effacement des 8 et 9 dans la 2-neuvine serait notée $2;9$-septine.

Il reste à savoir comment représenter les septines sous forme de spirale. Pour cela, il faut noter que les nombres effacés sont successifs et plus grands que n. Ce sont donc les derniers de la spirale. En outre l'effacement va les remplacer dans la n-spinine par les entiers qui les suivent dans la m-quenines. L'idée de représentation est donc d'écrire les nombres sur les rayons classiques de la spirale en omettant les successeurs des nombres effacés. Ces successeurs sont alors écrits en fin de rayon dans l'ordre des effacements. Cela fonctionne par exemple sur la dizine obtenue à partir de la 2-onzine : 1 → 6 3 10 5 9 7 8 4 2.

Nous détaillons plutôt la fabrication de la septine par effacement de la 2-neuvine :

1. Prenons $n = 7$.
2. Choisissons $m = 9$ ($m = 8$ serait le plus petit).
3. Fabriquons [9, 1, 8, 2, 7, 3, 6, 4, 5] la 2-neuvine ...
4. Et 1 → 9 5 7 6 3 8 4 2 l'orbite spiralique de 1.
5. Effaçons soit dans l'orbite de 1 le 8 et le 9, ils sont remplacés par 4 et 5 qui seront donc placés en fin de spirale.

La figure 5 montre deux réalisations de la septine, les $3;8$-septine et $2;9$-septine respectivement à partir de la 3-octine et de la 2-neuvine. Si la septine issue de l'octine possède bien une forme de spirale, l'effacement du 8 dans la permutation se transcrit par un simple effacement sur la spirale, on voit que celle issue de la neuvine, bien que toujours spiralique est malheureusement d'une esthétique plus discutable. En effet, il est nécessaire que "6, 7" et "4, 5" soient sur le même rayon mais pas dans un ordre croissant ...

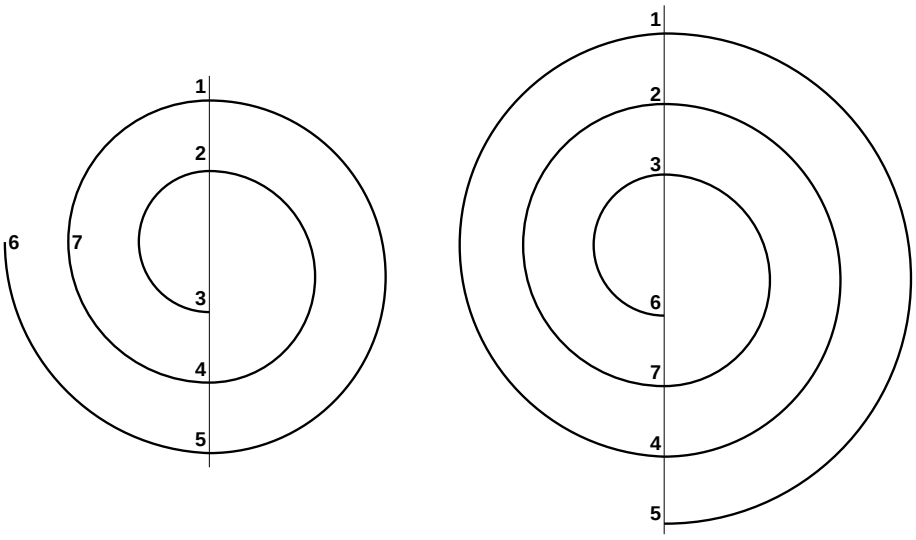

FIG. 5 – Septines, à partir de la 3-octine à gauche et de la 2-neuvine à droite.

Références

[Bringer, 1969] Bringer, M. (1969). Sur un problème de Raymond Queneau. *Mathématiques et sciences humaines*, 27 :13–20.

[Burton, 1998] Burton, D. M. (1998). *Elementary number theory*. International series in Pure and Applied Mathematics. McGraw-Hill, 4^{th} edition.

[Demazure, 1997] Demazure, M. (1997). *Cours d'algèbre. Primalité, Divisibilité, Codes*, volume XIII of *Nouvelle biliothèque Mathématique*. Cassini, Paris.

[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 et al., 2007] Dumas, J.-G., Roch, J.-L., Tannier, E., and Varrette, S. (2007). *Théorie des codes : Compression, Cryptage, Correction*. Dunod.

[Elliott and Murata, 1997] Elliott, P. D. T. A. and Murata, L. (1997). On the average of the least primitive root modulo p. *Journal of The london Mathematical Society*, 56(2) :435–454.

[Esposito-Farèse, 2000] Esposito-Farèse, G. (2000). Oulipian exercices (7). `http://www.iap.fr/users/esposito/oulipo7.html`.

[Lidl and Niederreiter, 1994] Lidl, R. and Niederreiter, H. (1994). *Introduction to Finite Fields and Their Applications*. Cambridge University Press, revised edition.

[Murata, 1991] Murata, L. (1991). On the magnitude of the least prime primitive root. *Journal of Number Theory*, 37(1) :47–66.

[Oliveira e Silva, 2000] Oliveira e Silva, T. (2000). Least primitive root of prime numbers. `http://www.ieeta.pt/~tos/p-roots.html`.

[Rosser and Schoenfeld, 1962] Rosser, J. B. and Schoenfeld, L. (1962). Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics*, 6 :64–94.

[Roubaud, 1969] Roubaud, J. (1969). Un problème combinatoire posé par la poésie lyrique des troubadours. *Mathématiques et sciences humaines*, 27 :5–12.

[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.

[Shoup, 1992] Shoup, V. (1992). Searching for primitive roots in finite fields. *Mathematics of Computation*, 58(197) :369–380.