EXPERIMENTAL FACTS ABOUT A LINEAR MAPPING.

EMMANUEL FERRAND

Abstract. These are some personal notes about a question raised by V.I. Arnold at his seminar in february 2005.

1. Introduction

A mapping from a finite set to itself can be described by a directed graph ("digraph") whose vertices are the elements of the finite set, with a directed edge between the vertices x and y iif y is the image of x by the mapping. This digraph might have several connected components. Each connected compoent consist in one cycle, adorned by some trees glued to its vertices.

Example of finite sets with natural mappings abounds. In [Ar], Arnold considered the dynamics of mapping of the from $x \to x^k$ acting on some finite groups. Among other things, he observed that the digraphs associated to such mappings show a *homogeneity property* : all the trees glued to a cycle are isomorphic.

Another class of finite sets are the finite dimensional vector spaces of finite fields. Their linear endomorphisms form a natural class of mappings to investigate. A particular case considered by Arnold is the following : let n be some integer, and consider the map $d = Id + S$ from $E = (\mathbb{Z}/2\mathbb{Z})^n$ to itself, where S is the circulant shift operator : $S(x_1, \ldots, x_n) = (x_n, x_1, x_2, \ldots, x_{n-1})$. Arnold has computed the associated digraph for $n = 1, \ldots, 12$ and observed an homogeneity property similar to the one mentioned above in the case of groups.

The experimental facts reported in these personal notes concern essentially the *maximal length* $L(n)$ of a cycle in the digraph, and its (mysterious) relationship with the parameter n. On can prove that $L(2^k) = 1$ for all $k \in \mathbb{N}$, that $L(2^k m) = 2^k.L(m)$ for $m > 1$ odd. Also $L(n)$ is the minimal period of the (eventually periodic) sequence $d^k, k \in \mathbb{N}$. On can also prove that for odd n, d acts as a bijection on the set of cardinality 2^{n-1} of vectors with an even number of nonzero coordinates.

2. Maximal cycle length

The numerical data presented below is compatible with the computations made by others ([Un],[OEIS, Si]).

n	1	2	3	4	5	6	7	8
$L(n)$	1	1	3	1	15	6	7	1
$L(n)/n$	1		1		3	1	1	
$(2^{(n-1)} - 1)/L(n)$	0	1	1	*	1	*	9	*

Date: 12 mars 2005.
1991 *Mathematics Subject Classification.* Primary 05C20.
Key words and phrases. Linear mapping, finite fields, iterations .

n	9	10	11	12	13	14	15	16
$L(n)$	63	30	341	12	819	14	15	1
$L(n)/n$	7	3	31	1	63	1	1	
$(2^{(n-1)}-1)/L(n)$			3		5			

n	17	18	19	20	21	22	23	24
$L(n)$	255	126	9709	60	63	682	2047	24
$L(n)/n$	15	7	511	3	3	31	89	1
$(2^{(n-1)}-1)/L(n)$	257		27				2049	

n	25	26	27	28	29	30	31	32
$L(n)$	25575	1638	13797	28	475107	30	31	1
$L(n)/n$	1023	63	511	1	16383	1	1	
$(2^{(n-1)}-1)/L(n)$					565		34636833	

n	37	41	43	47
$L(n)$	3233097	41943	5461	8388607
$L(n)/n$	87381	1023	127	178481
$(2^{(n-1)}-1)/L(n)$	21255	26214425	805355523	8388609

It is observed in [Un] that, for odd n, $L(n)/n$ is, in these tables, always of the form 2^j-1, except for $n=23$. I observed that, in these tables, when n is prime, $2^{n-1}-1$ is decomposed as a product $L(n)R(n)$, with $gcd(L(n),R(n))=1$ except when $n=37$. Furthermore the powers of n in the prime decompositions of $L(n)$ and $2^{(n-1)}-1$ are the same.

3. When 2 is replaced by other primes

The same mapping, but in $\mathbb{Z}/3\mathbb{Z}$.

n	3	5	7	11	13	17
$L(n)$	1	40	182	242	26	27880
$L(n)/n$		8	26	22	2	1640
$(3^{(n-1)}-1)/L(n)$		2	4	244	20440	1544

The same mapping, but in $\mathbb{Z}/5\mathbb{Z}$.

n	3	5	7	11	13
$L(n)$	12	1	868	3124	312
$L(n)/n$	4		124	284	24
$(5^{(n-1)}-1)/L(n)$	2		18	3126	782502

We observe that $5^{12}=1+782502\cdot 312$, but that $gcd(782503,312)=6$.

The same mapping, but in $\mathbb{Z}/13\mathbb{Z}$.

n	3	5	7
$L(n)$	12	420	84
$L(n)/n$	4	84	12
$(13^{(n-1)}-1)/L(n)$	14	68	57462

In $\mathbb{Z}/11\mathbb{Z}$, for $n=7$ we obtain the decomposition $11^6=1+1332\cdot 1330$.

References

[Ar] Arnold',V.I. *The topology of algebra: combinatorics of squaring.* Funktsional. Anal. i Prilozhen. 37 (2003), no. 3, 20–35, 95; translation in Funct. Anal. Appl. 37 (2003), no. 3.

[OEIS] *Online encyclopedia of integer sequences*, sequence A038553. www.research.att.com

[Si] Simmons, G.J. *The structure of the differentiation digraphs of binary sequences.* Ars Combin. 35 (1993), A, 71–88.

[Un] Unknown author, *Bit-string orbits under rotate XOR*, www.mathpages.com

Institut Fourier, BP 74, 38402 St Martin d'Hères Cedex, France.
E-mail address: `emmanuel.ferrand@ujf-grenoble.fr`