

## SOLVING SOME TILING PROBLEMS WITH POLYNOMIALS

*Abstract:* Following other people's ideas on 'tiling the line', the author tries to make use of the convenient tool of polynomials over various structures. This enables to define several species of 'polynomial tilings', may give new insight on solved but complicated problems (such as HAJÒS theorem) and even provides with elegant solutions to recent conjectures.

*Keywords:* tiling, mosaics, rythmic canons, VUZA canons, JOHNSON's problem.

**Introduction.** The ideas exposed here made the bulk of a communication to the MaMux seminar at IRCAM on the 9 of february, 2002.

Having perused preprints from Messrs FRIPERTINGER and TANGIAN (also speakers in the same meeting), one of which made use of the MÖBIUS inversion and the other putting forward a polynomial formulation of Tom JOHNSON's problem, I was tempted to explore in greater detail the advantages of using the considerable mathematical knowledge about polynomials to explore tiling problems in the field of rythmic canons.

Several ideas are just ideas – more or less promising – but some of them proved worth their while. Consequently I will mention some unfinished bits of work when I feel they deserve it.

### 1. TOM JOHNSON'S PROBLEM.

#### 1.1. Polynomial formulation.

It is elsewhere related how Andranik TANGIAN expressed the problem of tiling the line with the rhythmic pattern (1 1 0 0 1) and its augmentations 'without gap or double beat' as a diophantine equation in polynomials :

$$A(X)J(X) + B(X)J(X^2) + C(X)J(X^4) = 1 + X + X^2 + \dots + X^{n-1} \quad (1)$$

where  $J(X) = 1 + X + X^4$  represents JOHNSON's pattern and  $A, B, C$  are polynomials with 0 or 1 as only coefficients and represent the schedule of voices entries.

My very first idea was that factorisations of the polynomial

$$\Delta_n(X) = 1 + X + X^2 + \dots + X^{n-1} \quad (2)$$

in factors with integer coefficients are very well known: the irreducible factors are the **cyclotomic polynomials**, discussed in greater detail below. This factorization approach looked rewarding only when the left-hand side of (1) reduces to a single product=  $A.J = \Delta_n$ .

#### 1.2. A conjecture.

Both Tom JOHNSON and Andranik TANGIAN noticed that empirical (or computerised) solutions of (1) have lengths that are multiples of 15. Indeed, the number of solutions with length  $15k$  is a rapidly increasing function of  $k$  :

$$S(1) = 1 \quad S(2) = 6 \quad S(3) = 20 \quad S(4) = 97 \quad \dots$$

We will show here how the polynomial approach allows to prove this JOHNSON-TANGIAN conjecture :

**Théorème 1.** *Any tiling of the line by the pattern 11001 and its binary augmentations (eg 101000001, 1000100000000001 ... ) has a length that is a multiple of 15.*

$J(X) = 1 + X + X^4$  will henceforth be called **Johnson's polynomial**. A finite field with  $q$  elements will be denoted  $\mathbb{F}_q$ . The gist of the proof is to read the identity (1) in the ring  $\mathbb{F}_2[X]$  of polynomials with 0-1 coefficients, setting  $1 + 1 = 0$ .

**Lemme 1.**  *$J$  is irreducible over  $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ .*

Meaning from now on  $J$  as an element of  $\mathbb{F}_2[X]$  (any identity in  $\mathbb{Z}[X]$  gives a new one in  $\mathbb{F}_2[X]$ ), though the converse is not true).

*Proof.* Easy by testing factors: clearly there are no factors of degree 1 (no root), hence any factorisation would be with (irreducible) factors like  $X^2 + aX + b$ ,  $a, b \in \mathbb{F}_2$ . But the only irreducible polynomial of degree 2 over  $\mathbb{F}_2$  is  $X^2 + X + 1$ , and it does not divide  $J$ .  $\square$

The reason behind the reason is that a root of  $X^2 + X + 1$  (in  $\mathbb{F}_4$ , the finite field with 4 elements) would be a cubic root  $\alpha$  of unity, hence clearly not a root of  $J$ : one would get  $2\alpha + 1 = 0 + 1 = 0$ , impossible (the characteristic of the field is still 2!).

**Lemma 2.**  $\mathbb{K} = \mathbb{F}_2[X]/(J)$  is the field with 16 elements.

*Proof.* A classical result: the ideal  $J$  is maximal in the ring  $\mathbb{F}_2[X]$  because  $J$  is irreducible. Hence the quotient is a field, isomorphic as a vector space (over field  $\mathbb{F}_2$ ) to the polynomials of degree at most 3 (as any polynomial modulo  $J$  has one and only one representation as a polynomial of degree  $< 4$ , by euclidian division). This set has clearly  $2^4 = 16$  elements, with 2 choices for each of the four coefficients.  $\square$

Thus we achieved a construction of a field  $\mathbb{K}$  where  $J$  has a root  $\alpha$  (indeed, more than one: see Lemma 5 where it is proven that the others are  $\alpha^2, \alpha^4, \alpha^8$ ).

(NB: for non mathematicians, the field  $\mathbb{K}$  above is just the set of polynomials in  $\alpha$ , where we set precisely  $J(\alpha) = \alpha^4 + \alpha + 1 = 0$ . The Lemma states that this is a field, that is to say any non-zero element has an inverse for multiplication).

**Lemma 3.** Any non zero element  $x \in \mathbb{K}^*$  fulfills  $x^{15} = 1$ .

This is LAGRANGE theorem on the multiplicative (abelian) group  $\mathbb{K}^*$ , which has 15 elements, or a form of FERMAT's (little!) theorem.

The following lemma is not necessary, but it helps understanding precisely where we stand.

**Lemma 4.** Any root of  $J$  (in  $\mathbb{K}$ ) is exactly of order 15.

*Proof.* The order of an element of group  $\mathbb{K}^*$  must be a divisor of 15 (by Lagrange's theorem). Say  $\alpha^3 = 1$ ; then plugging in  $J(\alpha) = 0$  gives (remembering  $1 + 1 = 0$  in  $\mathbb{K}$ )

$$0 = \alpha^4 + \alpha + 1 = 2\alpha + 1 = 1 \quad \text{contradiction}$$

The other case  $\alpha^5 = 1$  is impossible too:

$$0 = \alpha^4 + \alpha + 1 = \alpha^{-1} + \alpha + 1 = \alpha^{-1}(1 + \alpha + \alpha^2) = (\alpha^3 - 1)\alpha^{-1}(\alpha - 1)^{-1}$$

hence  $\alpha$  would be also of order 3! So the only possibility is that  $\alpha$  is of order 15 (by the way  $\mathbb{K}^* \approx \mathbb{Z}/15\mathbb{Z}$ , not that it matters here).  $\square$

**Lemma 5.** If  $\alpha$  is a root of  $J$  (in  $\mathbb{K}$ ) then so are  $\alpha^2, \alpha^4, \dots, \alpha^{2^k}$ .

*Proof.* Easy enough: say  $\alpha^4 = -\alpha - 1 = \alpha + 1$  (remember,  $-1=1$ !). Then

$$\alpha^8 = (\alpha + 1)^2 = \alpha^2 + 1 \quad \text{which is to say} \quad J(\alpha^2) = 0$$

This is now also true for  $\alpha^{2^k}$  by immediate induction.  $\square$

Indeed, by this lemma, the roots of  $J$  ARE  $\alpha, \alpha^2, \alpha^4$  and  $\alpha^8$  (all different elements of order 15) (notice  $\alpha^{16} = \alpha$  and hence  $\alpha^{2^k} = \alpha^{2^{k \pmod{4}}}$ ) and so are the roots of  $J(X^2)$ , because by a straightforward verification, in  $\mathbb{F}_2[X]$

$$J(X^2) = J(X)^2 \quad J(X^{2^k}) = J(X)^{2^k} \quad (X \mapsto X^2 \text{ is the famous Frobenius automorphism})$$

*Proof.* We now end the proof of the theorem.

Suppose there is a tiling of length  $n$ , e.g. there exists polynomials  $A, B, C \dots$  (with 0-1 coefficients) fulfilling

$$A(X)J(X) + B(X)J(X^2) + C(X)J(X^4) + \dots = \Delta_n(X) = 1 + X + X^2 + \dots + X^{n-1}$$

Let us substitute  $X = \alpha$ , a root of  $J$  in  $\mathbb{K}$ . This makes sense as an identity in  $\mathbb{Z}[X]$  may be quotiented to  $\mathbb{F}_2[X] \subset \mathbb{K}[X]$ . Indeed by force of the particular problem we are studying, the coefficients of all

polynomials involved are already 0's and 1's. The left-hand term vanishes by Lemma 5 (for any number of augmentations). So

$$0 = \Delta_n(\alpha) = (\alpha^n - 1)(\alpha - 1)^{-1}$$

Hence  $\alpha^n - 1 = 0$  and  $n$  must be a multiple of the order of  $\alpha$  (this is a classical property of the order of an element in a group): by Lemma 4, the proof is now complete.  $\square$

*For the reader: Adapt the proof supra for the polynomial  $1 + X + X^3$  and prove that any solution of this variant of the Johnson's problem has a length multiple of 7 (and hence of 21, as any tile is of length 3).*

## 2. CYCLOTOMIC POLYNOMIALS

### 2.1. A simpler tiling problem.

Let us return to the fundamental problem of tiling the line, or of rhythmic canons. We consider hereafter the following problem:

Find two subsets  $A, B$  of  $M = \{0, 1, \dots, n - 1\}$  for which

$$(A, B) \rightarrow M \quad (a, b) \mapsto a + b$$

is one-to-one and onto. If  $A$  is a pattern (e.g. 1 1 0 0 1) and  $B$  an entry-table, this represents a canon, with copies of  $A$  translated by the action of  $B$  making up the tiles of the tiling.

The polynomial translation of this is:

**Problem 1.** Find two polynomials  $P, Q$  with coefficients in  $\{0, 1\}$  for which

$$P \times Q = \Delta_n$$

The correspondence between subsets and polynomials is straightforward, e.g.  $P = \chi_A = \sum_{i \in A} X^i$ .

This kind of 'characteristic polynomial' (like characteristic functions of a set) reminds of VUZA [V4] and leads to very difficult mathematical problems. In this simple case, it reminds one of the adjacency matrix of a graph.

### 2.2. 0-1 factors.

Now we must factor  $\Delta_n$  as a product of two '0-1 polynomials'. The general solution of this is not known, but the polynomial formulation helps to tackle the matter.

In my talk I tried to stress the point that the set  $\aleph$  of all 0-1 polynomials is worth considering, though it suffers from terrible flaws: it is not closed under the usual composition laws  $(+, \times, \circ)$ , that is to say a combination of two 0-1 polynomials is not necessarily another 0-1 polynomial (try adding one such polynomial with itself!)

Still it is an interesting set, the closest indeed to the problem of tiling the line and its study should perhaps be considered. On the one hand, it branches to excellent and well-known structures (such as  $\mathbb{Z}[X], \mathbb{F}_2[X], \mathcal{P}(\mathbb{N})$  – the set of subsets of  $\mathbb{N}$ ) with satisfying morphisms [my proof of JOHNSON-TANGIAN conjecture relies heavily on the arrow  $\aleph \rightarrow \mathbb{F}_2[X] \subset \mathbb{F}_{16}[X]$ ]; on the other, some concepts may be adapted and studied in  $\aleph$ , such as divisibility, ideals, aso. Such results as I have found in this direction are still scarce, as of now, and I won't show them yet.

One line of thought that does reap some interesting rewards is to consider  $\aleph$  as a subset of  $\mathbb{Z}[X]$ . In this ring, the ultimate factorization of  $\Delta_n$  is known and the (irreducible) factors are very close to  $\aleph$ : indeed many of them are IN  $\aleph$ . I state the following classical results without proof, they should be found in any classical textbook in commutative algebra.

**Théorème 2.** The irreducible factors in  $\mathbb{Z}[X]$  or  $\mathbb{Q}[X]$  of  $\Delta_p$  are the cyclotomic polynomials

$$\Phi_n(X) = \prod_{d < n, d \wedge n = 1} (X - \xi^d) = \prod_{d < n, d \wedge n = 1} (X - e^{2id\pi/n})$$

where  $n$  is any divisor of  $p$  (greater than 1).

The degree of  $\Phi_n$  is given by EULER totient function, it is the number of integers relatively prime to  $n$ , that is to say the regular (multiplicative) elements of the ring  $(\mathbb{Z}_n, +, \cdot)$  or the generators (additively) of the group  $(\mathbb{Z}_n, +)$ .

Notice that the cyclotomic polynomials  $\Phi_n$  are monic polynomials, with integer coefficients. Indeed usually most of the coefficients are 0's or  $\pm 1$ 's.

Here are some examples :

- $\Phi_p = \Delta_p = 1 + X + X^2 + \dots + X^{p-1}$  for any prime  $p$
- $\Phi_4 = 1 + X^2$      $\Phi_8 = 1 + X^4$      $\Phi_9 = 1 + X^3 + X^6$      $\Phi_{25} = 1 + X^5 + X^{10} + X^{15} + X^{20}$
- $\Phi_{12} = 1 - X^2 + X^4$      $\Phi_{24} = 1 - X^4 + X^8$      $\Phi_{42} = 1 + X - X^3 - X^4 + X^6 - X^8 - X^9 + X^{11} + X^{12}$
- $\Phi_{99} = 1 - X^3 + X^9 - X^{12} + X^{18} - X^{21} + X^{27} - X^{30} + X^{33} - X^{39} + X^{42} - X^{48} + X^{51} - X^{57} + X^{60}$
- $\Phi_{100} = 1 - X^{10} + X^{20} - X^{30} + X^{40}$

### 2.3. Using the cyclotomic polynomials for the construction of canons.

As one will easily see, many cyclotomic polynomials are indeed 0-1 polynomials and readily provide canons (though not necessarily tilings of the line) by product. For instance

**Proposition 1.** *The product  $\Phi_{p^k}\Phi_{q^l}$  is always a 0-1 polynomial (i.e. a canon, with holes, but without overlapping).*

As these are irreducible factors, any factorisation of  $\Delta_n$  in the product of two polynomials with integer coefficients, and hence in 0-1 polynomials, must be a partition of the canonic factorization  $\Delta_n = \prod_{1 < d|n} \Phi_d$ . Hence

**Théorème 3.** *Any factorization  $\Delta_n = P.Q$  in  $\mathbb{Z}[X]$  is such that  $P = \prod_{i \in I} \Phi_j$  and  $Q = \prod_{j \in J} \Phi_j$  where  $(I, J)$  is a partition of the set of divisors of  $n$  (1 excluded).*

Set for instance  $n = 15$ : then a very simple rhythmic canon is (1 1 1) repeated 5 times, ie

$$\Delta_{15} = (1 + X + X^2)(1 + X^3 + X^6 + X^9 + X^{12}) = \Phi_3 \times (\Phi_5 \times \Phi_{15})$$

This simple result has many interesting consequences :

- With a table of cyclotomic polynomials, it is a simple matter to find all factorizations in 0-1 polynomials by way of a computer search. This can (and will) be bettered with some pruning of the binary tree of all possible partitions.
- (just illustrating the power of the notion) Tom Johnson mentioned the case of the pattern (0 3 7 11 31) and the difficulty of knowing whether it tiles the line (JOHNSON considered a more general notion of 'tiling loops', see his paper here).

From a look at the roots (in the complex field) of the polynomial  $1 + X^3 + X^7 + X^{11} + X^{31}$  (one of which is for example  $1.04200725545 + 0.1323321581i$ , and the only real one being  $-0.8339814982286$ ) neither of which lies on the unit circle, it is obvious that this cannot be a product of cyclotomic polynomials; hence it can't be a factor of any  $\Delta_n$ , for any  $n$ , meaning the pattern won't tile any line.

- Easier: by the same line of reasoning, the 'JOHNSON's polynomial'  $1 + X + X^4$  cannot tile the line by itself (the roots are either smaller or greater than 1). The more complicated problem of tiling the line with it and a number of its augmentations does have solutions as JOHNSON and TANGIAN have found, but of course it is much more difficult to prove in the abstract!

## 3. VUZA CANONS AND POLYNOMIAL TILINGS

### 3.1. Of some polynomial canons.

The notion of VUZA canons, or as he put it 'regular complementary of maximal category', is now more or less common knowledge [V,A]. The polynomial approach enables to look for special species of canon, by simply factoring  $\Delta_n$  in cyclotomic polynomials and trying all the recombinations to get all possible rhythmic canons :

**Définition 1.** *A polynomial canon of length  $n$  is simply a solution of  $P \times Q = \Delta_n$ ,  $P$  and  $Q$  being 0-1 polynomials.*

**Définition 2.** *An aperiodic canon is a polynomial canon in which neither  $P$  nor  $Q$  are 'periodic', meaning  $P$  (resp.  $Q$ ) won't satisfy any relation of the kind  $P(X) = P_1(X^k)$  for some  $k > 1$ .*

**Définition 3.** *An irreducible (polynomial) canon is a canon for which neither  $P$  nor  $Q$  is reducible, e.g. one excludes that  $P = R \circ S$*

(here is an example of a reducible polynomial :

$$R(X) = 1 + X^2 \quad S(X) = X + X^3 \quad P(X) = R(S(X)) = 1 + S(X)^2 = 1 + X^2 + 2X^4 + X^6$$

Now the first definition is too general, the last too restrictive, the middle one should be just right. Unfortunately computer searching has so far failed to reveal any. Theoretical arguments show that if a solution exists of length  $n$ , then  $n$  must be a rather heavily composite number (because of HAJOS/VUZA theorem, see below).

But hope remains, insofar as

**Proposition 2.** *In any polynomial canon, at most one of the factors  $P, Q$  is periodic.*

*Proof.* Suppose  $P$  (resp.  $Q$ ) is  $p$ -periodic (resp.  $q$ -periodic) and  $P.Q = \Delta_n$ . Then necessarily  $P(X) = 1 + X^{kp} + \dots$  and  $Q(X) = 1 + X^{lq} + \dots$  and  $P.Q = 1 + X^{\inf(kp, lq)} + \dots$  cannot be equal to  $\Delta_n = 1 + X^1 + X^2 + \dots$  [the special case  $kp = lq$  being worse].  $\square$

### 3.2. Non metronomic canons.

Some interesting canons DO exist, anyway, for

$$n = 16, 24, 32, 36, 40, 48, 54, 56, 60, 64, 72, 80, 81, 84, 88, 90, 96, 100, 104, 108, 112, 120, \dots$$

I define here this new species :

**Définition 4.** *A non metronomic canon is a polynomial canon in which neither factor is of the form  $\Delta_d(X^\ell) = 1 + X^\ell + X^{2\ell} + \dots + X^{d\ell}$ .*

The term ‘non-metronomic’ is self-explanatory. Some examples : for  $n = 24$  the solutions are

$$\begin{array}{ll} 1 + X + X^4 + X^5 & 1 + X^2 + X^8 + X^{10} + X^{16} + X^{18} \\ 1 + X + X^2 + X^6 + X^7 + X^8 & 1 + X^3 + X^{12} + X^{15} \\ 1 + X + X^4 + X^5 + X^8 + X^9 & 1 + X^2 + X^{12} + X^{14} \\ 1 + X^2 + X^4 + X^{12} + X^{14} + X^{16} & 1 + X + X^6 + X^7 \end{array}$$

and the four dual solutions (reversing the roles of the two factors). Let us remind the reader that, for instance, the last solution means the pattern (0 1 6 7) e.g. (X X - - - X X) with the entry table (0 2 4 12 14 16).

These canons are numerous, from the last Proposition it is possible at least to arrange for the rhythmic pattern to be irregular, so I think this is a useful dingo for composers.

In the last examples, either the entry table or the rhythmic pattern is regular (though non metronomic), hence this is not a VUZA canon. Generally speaking, there is a hierarchy :

**Proposition 3.** *Any irreducible polynomial canon is aperiodic. Any aperiodic canon is irregular, and is a VUZA canon.*

The reverse of the last sentence is not true : an aperiodic canon provides a tiling of the **integer range**  $\{0, 1, 2, \dots, n - 1\}$ , while a VUZA canon tiles  $\mathbb{Z}/n\mathbb{Z}$ . That means that an aperiodic canon is (would be) a tight kind of VUZA canon. Hence, too, it is useless to look for such canons of length

$$n = p^\alpha, p^\alpha q, p^2 q^2, pqr, pqrs, \dots$$

and generally speaking all the cases mentioned in (both) HAJOS and VUZA’s theorems.

I have found direct demonstrations of the impossibility of (most of) such  $n$ ’s, using only simple properties of cyclotomic polynomials. Let us mention one of these demonstrations as an example : I think it helps getting a better understanding of why such lengths are forbidden.

### 3.3. The case of $n = p^\alpha q$ .

Factors of  $\Delta_n$  are  $\Phi_p, \Phi_q, \Phi_{pq}, \Phi_{p^2 q}, \dots, \Phi_{p^\beta q} \dots$ . I state some formulas :

$$\Phi_{p^\beta q}(X) = \Phi_{pq}(X^{p^{\beta-1}}) = 1 - X^{p^{\beta-1}} + \dots + X^{(p-1)(q-1)p^{\beta-1}}. \quad \Phi_{p^k}(X) = \sum_{i=0}^{p-1} X^{ip^{k-1}}$$

The first one comes from a more general identity:  $\Phi_{p^k q^\ell}(X) = \Phi_{pq}(X^{p^{k-1}q^{\ell-1}})$ , which follows from the WONDER formula (W)

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)} \quad (W)$$

it being the MÖBIUS inversion of the factorization of  $\Delta_n$ .

Now in a factorization of  $\Delta_n = A \times B$ ,  $\Phi_{pq}$  is a factor of (say)  $P$ , and so may be  $\Phi_p$  or  $\Phi_q$ .

- If it is not so, then  $\Phi_{pq} \mid P$  and  $\Phi_p \cdot \Phi_q \mid Q$ , the other factors being the  $\Phi_{p^\beta q}$  (all are polynomials in  $X^p$  by the preceding Lemma). But then  $Q$  must be wrong:

$$Q(X) = \Phi_p(X)\Phi_q(X) \times R(X^p) = (1 + 2X + \dots)(1 + kX^p + \dots) = 1 + 2X + \dots$$

and this is not a 0-1 polynomial.

- Say  $P$  contains the factors  $\Phi_{pq}$  and  $\Phi_q$  together: then  $P$  admits the factor  $\Phi_{pq} \cdot \Phi_q = 1 + X^p + \dots + X^{p(q-1)}$  (see (W)), and we get two subcases:
  - $\Phi_p$  also divides  $P$ : then  $Q$  is only a product of the  $\Phi_{p^\beta q}$ 's and hence a polynomial in  $X^p$ ,
  - $\Phi_p$  divides  $Q$ , but not  $P$ : then  $P$  is a polynomial in  $X^p$ , as are all its factors.
- Last case:  $\Phi_{pq} \cdot \Phi_p = \Phi_p(X^q)$  (see (W))  $1 + X^q + \dots + X^{q(p-1)} \mid P$ , hence

$$P(X) = \Phi_p(X^q) \cdot S(X^p) \text{ while } Q(X) = \Phi_q(X) \times R(X^p) = (1 + X + X^2 + \dots + X^{q-1})R(X^p)$$

But the remaining polynomials  $R$  and  $S$  (in  $X^p$ ) are made of

$$\Phi_{p^\beta q}(X) = \Phi_{pq}(X^{p^{\beta-1}}) = (1 - X^{p^{\beta-1}} + \dots) \quad \beta \geq 1$$

Hence  $S(X^p) = 1 - X^{p^{\beta-1}} + \dots$  for some  $\beta \geq 1$ , and  $P$  is not a 0-1 polynomial as  $P(X) = (1 + X^q + \dots) \times (1 - X^{p^{\beta-1}} + \dots)$  and  $q$  cannot be equal to  $p^{\beta-1}$ .

#### 4. BETWEEN VUZA-CANONS AND APERIODIC CANONS.

A general Vuza-canons 'of order  $n$ ' stretches over the range  $0 \dots n$ . Here is one of the shorter examples, for  $n = 72$  (computed by ANDREATTA [A]):

$$(1 + x^8 + x^{16} + x^{18} + x^{26} + x^{34})(1 + x + x^5 + x^6 + x^{12} + x^{25} + x^{29} + x^{36} + x^{42} + x^{48} + x^{49} + x^{53})$$

This product outpasses  $x^{72}$  of course; one has to apply a reduction modulo 72 on the degrees to get  $\Delta_{72}$ . The rule would be

$$\text{IF } p \geq 72 \text{ THEN } x^p \rightarrow x^{p-72}$$

It can be formalized more prettily by euclidean division: one expands the product, then takes it modulo  $x^{72} - 1 = (x - 1)\Delta_{72}$  (that is to say, divide by  $x^{72} - 1$  and take the remainder).

Hence a characterization of VUZA canons, that may help to get at them from a theoretical point of view:

**Prop.** *There exists a Vuza-canon of order  $n$  iff it is possible to write the following identity between the 0-1 polynomials  $A, B, Q$ :*

$$A \times B = (x^n - 1) \times Q + \Delta_n = ((x - 1)Q + 1)\Delta_n$$

The only point of note is that  $Q$  is necessarily a 0-1 polynomial, which is easy to prove (in the example above,

$$\begin{aligned} A &= X^{34} + X^{26} + X^{18} + X^{16} + X^8 + 1 \\ B &= X^{53} + X^{49} + X^{48} + X^{42} + X^{36} + X^{29} + X^{25} + X^{12} + X^6 + X^5 + X + 1 \\ P &= X^{87} + X^{83} + X^{82} + X^{79} + X^{76} + X^{75} + X^{74} + X^{71} + X^{70} + X^{69} + \dots \\ &+ \dots \text{ (all the } X^k \text{ in this range are here)} + X^{13} + X^{12} + X^9 + X^8 + X^6 + X^5 + X + 1 \\ Q &= X^{15} + X^{11} + X^{10} + X^7 + X^4 + X^3 + X^2 \\ 1 + Q \cdot (X - 1) &= X^{16} - X^{15} + X^{12} - X^{10} + X^8 - X^7 + X^5 - X^2 + 1 \end{aligned}$$

In this formula,  $A, B, Q$  are 0-1 polynomials and  $(x - 1)Q + 1$  is a difference of 0-1 polynomials ( $1 + xQ$  minus  $Q$ ), and all the cyclotomic polynomials that make up  $\Delta_n$  must be factors of  $A$  or  $B$ .

This proposition suggests that factorizations of  $\Delta_n$  (maybe in adequate finite rings) could be the key to a real understanding of VUZA-canons.