A solution to Johnson-Tangian conjecture

A recent problem in musical tilings of the line arose when TANGIAN [T] devised a computerized solution to JOHNSON's problem [J], that is, tiling the line with the pattern 11001. All the solution appeared to have a length that is a multiple of 15 (and indeed solutions were found for all multiples up to computational limits). Is this general ? If so, why ?

Though A. Tangian imagined a polynomial representation of this problem just in order to explain why it was probably too difficult to solve algebraically, ironically enough it provided the means by which I managed the proof of the following

Theorem. *Any tiling of the line by the pattern* 11001 *and its binary augmentations*

(eg $101000001, 10001000000000001\dots$) has a length that is a multiple of 15.
As shown by [T],

Lemma 1. *The problem of tiling is equivalent to solving a diophantine equation in polynomials with 0-1 coefficients:*

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

$J(X) = 1 + X + X^4$ will henceforth be called **JOHNSON's polynomial** – he richly deserves it.

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

Meaning J as an element of $\mathbb{F}_2[X]$.

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.*

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 α 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 3. *$\mathbb{K} = \mathbb{F}_2[X]/(J)$ is a 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.*

Thus we achieved a construction (of $\mathbb{F}_{16}$, the one and only field with 16 elements, but it's neither here nor there) of a field where J has a root (indeed, more than one) α.

Lemma 4. *Any non zero element $x \in \mathbb{K}^*$ fulfills $x^{15} = 1$.*

This is LAGRANGE's theorem on the multiplicative (abelian) group $\mathbb{K}^*$, which has 15 elements, or a form of FERMAT's (little !) theorem. A short proof: for any given $x \in \mathbb{K}^*$, the sets

$$\mathbb{K}^* = \{1, a, b, \ldots\} \qquad \text{and} \qquad x\mathbb{K}^* = \{x, xa, xb, \ldots\}$$

are equal ($a \mapsto xa$ being one-to-one and onto). Hence the product of their respective elements is the same, e.g.

$$1.a.b.\ldots = (x.1)(x.a).(x.b).\ldots = x^{|\mathbb{K}^*|}(1.a.b.\ldots) = x^{15}.1.a.b.\ldots$$

and hence $x^{15} = 1$, qed.

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

Lemma 5. *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 $\mathbb{K}$)*

$$0 = \alpha^4 + \alpha + 1 = 2\alpha + 1 = 1 \qquad \textit{contradiction}$$

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

Lemma 6. *If alpha is a root of J (in $\mathbb{K}$) then so are $\alpha^2, \alpha^4, \ldots \alpha^{2^k}$.*

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

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

This is now also true for α^{2^k} by immediate induction.

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

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

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 probelm we are strudying, the coefficients of all polynomials involved are already 0's and 1's !!! The left-hand term vanishes by Lemma 6 (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 α (this is a classical property of the order of an element in a group): by Lemma 5, the proof is now complete.