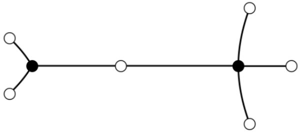
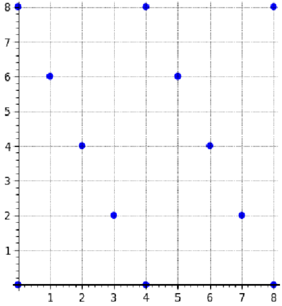
Factorisation of Belyi like polynomial over finite fields

Gabriel Soranzo

2022

Introduction





G. Belyi (1951-2001)

$$X^a(1-X)^b-1$$

Objectives

We are going to explain how factorising over finite fields $\mathbb{F}_p$ the polynomials $\mu_{a,b} = X^a(1-X)^b - 1$.

- They are already general algorithms for that! But:
- We are looking for an "understanding factorisation": what is the logic behind the scene
- We are looking for a "by hand" algorithm: no big resultant or gcd method

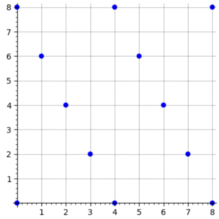
Why?

- Factorisation of $X^a(1-X)^b - 1$ over $\mathbb{F}_p$, why?
- Because it gives the factorisation of the Belyi polynomials $\beta_{a,b} = X^a(1-X)^b - \frac{(a+b)^{a+b}}{a^a b^b}$ over $\mathbb{F}_p$: as $\lambda_{a,b} = \frac{(a+b)^{a+b}}{a^a b^b}$ is in $\mathbb{F}_p$ the there is an integer k such that $\lambda_{a,b}^k = 1$ so that the factors of $\beta_{a,b}$ are in the factors of $\mu_{ka,kb}$.
  Why are we looking for factorisation of $\beta_{a,b}$ over $\mathbb{F}_p$?
- Because (with Hensel lemma and work on models) it can give factorisation of $\beta_{a,b}$ over $\mathbb{Q}_p$.
  Why are we looking for factorisation of $\beta_{a,b}$ over $\mathbb{Q}_p$?
- Because it can (with Krasner lemma) give the local Galois group of the Belyi polynomials $\beta_{a,b}$
  Why are we looking for the local Galois groups of $\beta_{a,b}$?
- Because it can maybe give (indication on) the global Galois group of $\beta_{a,b}$, and so on the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the vertices of the children drawing given by $\beta_{a,b}$.

Lattice associated to some irreducible polynomial

What is the main idea of the factorisation of the polynomials $\mu_{a,b} = X^a(1-X)^b - 1$?

➔ We are going to use lattices.



Main idea from factorisation of $X^n - 1$

How do we factor polynomial $\varphi_n = X^n - 1$ in $\mathbb{F}_p$?

Factorisation of $X^n - 1$

$$X^n - 1 = \prod_{k|n} \Phi_k$$

(This is in fact not an irreducible factorisation because the Φ are in general not irreducible in $\mathbb{F}_p$ but it is conveniente to give the idea.)

By associating to each cyclotomic polynomial Φ_k a 1-dimensional lattice $L_k = k\mathbb{Z}$ we can reformulate this by:

Factorisation of $X^n - 1$ - version 2

$$X^n - 1 = \prod_{n \in L_k} \Phi_k$$

Main idea: appication to $\mu_{a,b}$

The idea is to make the same thing as this new version factorisation theorem:

Factorisation of X^n-1 - version 2

$$X^n-1=\prod_{n\in L_k}\Phi_k$$

but with $\mu_{a,b}=X^a(1-X)^b-1$.
Difference between X^n-1 and $X^a(1-X)^b-1$: there is **2** parameters a and b.
So to each irreducible polynomial Φ of $\mathbb{F}_p$ a **2**-dimensional lattice L_Φ such that

Factorisation of $X^a(1-X)^b-1$

$$X^a(1-X)^b-1=\prod_{(a,b)\in L_\Phi}\Phi$$

Definition of the lattice

Let $P \in \mathbb{F}_p[X]$ an irreducible polynomial. We note L_P the following subset of $\mathbb{N}^2$:

$$L_P = \{(a, b) \in \mathbb{N}^2 \mid P | X^a(1-X)^b - 1\}$$

Let $x \in \overline{\mathbb{F}_p}$. We note L_x the following subset of $\mathbb{Z}^2$:

$$L_x = \{(a, b) \in \mathbb{Z}^2 \mid x^a(1-x)^b = 1\}$$

Fondamental observation

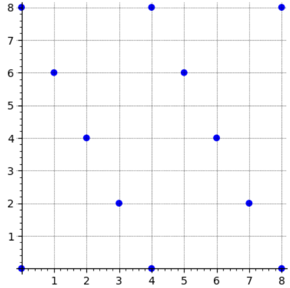
The subset L_x of $\mathbb{Z}^2$ is a lattice.

Second observation

For all x root of P we have $L_P = L_x \cap \mathbb{N}^2$.

An example

Here the example of the lattice associated to the polynomial Φ_4 in $\mathbb{F}_3$



Lattice associated to Φ_4 in $\mathbb{F}_3$

Factorisation of $X^a(1-X)^b-1$

In termes of lattices L_P we can reformulate the problem of the factorisation of $\mu_{a,b} = X^a(1-X)^b - 1$ in the following form:

Factorisation of $X^a(1-X)^b-1$

Find all the irreducible factors of $\mu_{a,b}$ is equivalent to find all the lattices L_P such that $(a, b) \in L_P$.

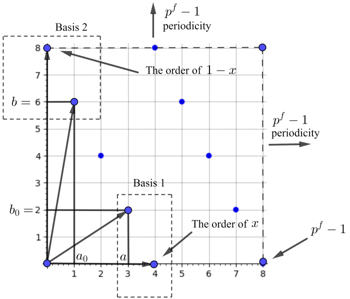
If we know all the lattices L_P, factoring the polynomials $X^a(1-X)^b-1$ comes down to an easy belonging to lattices problem.
The program is so the following:

Project

Find all the lattices L_P.

First properties of the lattices L_P

What does the lattices L_P look like?



We are going here to explain the order of x and p^f-1-periodicity.

The order of L_P

As it is well known all irreducible polynomial P is a factor of some cyclotomic polynomial Φ_k where we will call k the **order** of P. As a result, for all root x of P:

$$\begin{aligned}(a,0)\in L_P &\iff x^a=1\\ &\iff k|a\end{aligned}$$

hence $L_P\cap(\mathcal{O}x)=\mathrm{ord}(P)\mathbb{Z}$.
So we can find the order of P from its lattice: we call k the **order** of the lattice L_P.

Consequence

As a result, our method generalize the method of factorisation for the X^n-1:

$$\begin{aligned} & X^n-1 \in L_\phi \\ \iff & X^n(1-X)^0-1 \in L_\phi \\ \iff & X^n(1-X)^0-1 \in L_\phi \cap (Ox) \\ \iff & n \in \operatorname{ord}(\phi)\mathbb{Z} \end{aligned}$$

Hence, as we know, the factors of X^n-1 are all the irreducible polynomials of order dividing n.

Difference with the factorisation of $X^n - 1$

The situation is not so comfortable for the general case because contrary to the 1-dimensional case, we will see that not all lattices are of the form L_P. These sorts of lattices could be named the **effective lattices** (modulo p).
So the central question is:

Central question

How to find what lattices are effective?

We will see now a reason why not all lattices are effective through the definition of the degree of effective lattices.

The degree of L_x

Let x be some root of Φ_ℓ (ie $x \in \overline{\mathbb{F}_p}$ is of order ℓ) then $x \in \mathbb{F}_{p^f}$ with

$$f = \deg(\Phi_{\ell,i}) = \mathrm{ord}_\ell(p) = \inf\{q \text{ such that } \ell | p^q - 1\}$$

As the degree f only depends on ℓ and as ℓ can be seen on the lattice L_x (intersection with (Ox)) then the degree f can be read on the lattice L_x. So we can speak of the **degree** of L_x.

The degree of L_x: geometric view

What are the other geometric implication of the degree?
As the order of x is ℓ then $x^\ell = 1$ hence:

$$\begin{aligned}(a,b) \in L_x &\Rightarrow x^a(1-x)^b = 1\\ &\Rightarrow \forall q,\ x^a(1-x)^b \times x^\ell = 1\\ &\Rightarrow \forall q,\ x^{a+q\ell}(1-x)^b = 1\\ &\Rightarrow \forall q,\ (a+q\ell, b) \in L_x\end{aligned}$$

hence L_x is ℓ-periodic horizontally.
We do not know the order ℓ' of $1-x$ a priori. But with the same reasoning we will obtain that L_x is ℓ'-periodic vertically.
As x and $1-x$ are all in $\mathbb{F}_{p^f}^*$ hence ℓ and ℓ' divide p^f-1.
So globally the lattice L_x is p^f-1-periodic.

Consequence: not all lattices are effective

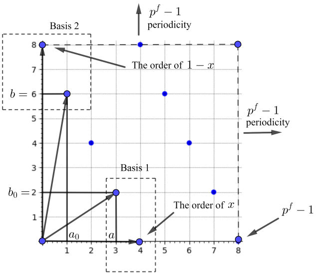
As said before not all lattices verify this property. If we take $v_1 = \begin{pmatrix} \ell \\ 0 \end{pmatrix}$ for the first vector basis for L_x, the p^f-1-periodicity constrains $v_2 = \begin{pmatrix} a \\ b \end{pmatrix}$ to verify $b | p^f - 1$ which is not the case for all lattices.

Example

With $p = 3$. Consider the lattice L generates by the vectors $v_1 = \begin{pmatrix} 4 \\ 0 \end{pmatrix}$ and $v_2 = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$. The degree associated to the order $k = 4$ is $f = 2$ because $4 | p^2 - 1$ and $4 \nmid p - 1$. But $3 \nmid p^2 - 1$.

Find lattices of given order o

How to find all the lattice of a given order o?



We have seen that $L_x \cap (Ox) = \mathrm{ord}(x)\mathbb{Z}$ and the p^f-1 periodicity: Let's understand b_0 and a.

Step 1: The minimal ordinate - Definition

We want to find what lattices are effective and more precisely, given an order $o \in \mathbb{N}$, find all the lattices L_x where $\mathrm{ord}(x) = o$ ie all effective lattices L such that $L \cap (Ox) = o\mathbb{Z}$.
Let $v_1 = \begin{pmatrix} o \\ 0 \end{pmatrix}$ and $v_2 = \begin{pmatrix} a \\ b_0 \end{pmatrix}$ be vector of L_x with b_0 is positive minimal. They will be a basis for L_x.
In this section we will obtain the number b_0 which could be name the **minimal ordinate**.

Step 1: The minimal ordinate - To the formula

- For example if $o = p^f - 1$ ie $L = L_x$ with x primitive. Then here $b_0 = 1$ because we can find the number a such that $x^a(1-x) = 1 \iff x^a = \dfrac{1}{1-x}$ (because x is primitive).
- In general for an order $o | p^f - 1$ we have $G_x = \langle x \rangle$ is equal to $K_o = \{y \in (\mathbb{F}_{p^f})^* \mid y^o = 1\}$. The number b is the smallest number such that $\left(\dfrac{1}{1-x}\right)^b \in G_x$ ie such that $(1-x)^b \in G_x$ ie such that $(1-x)^{bo} = 1$ ie such that $\operatorname{ord}(1-x) | bo$

Step 1: The minimal ordinate - The formula

We've seen, with $o' = \mathrm{ord}(1-x)$ that

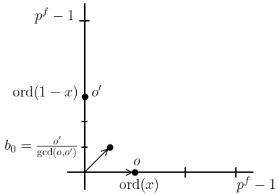
$$b_0 = \inf\{b \text{ such that } o' \mid bo\}$$

as a result

Formula for b_0

The minimal positive ordinate for a effective lattice of order o is

$$b_0 = \frac{\mathrm{lcm}(o, o')}{o} = \frac{o'}{\gcd(o, o')}$$



Step 1: The minimal ordinate - Consequences

As a result

- If $\text{ord}(1-x)|\text{ord}(x)$ ie $o'|o$ (for example if x is primitive ie $\text{ord}(x)=p^f-1$) then $\mathrm{lcm}(o,o')=o$ so that $b_0=\frac{\mathrm{lcm}(o,o')}{o}=\frac{o}{o}=1$.
- If o' and o are coprime then $\mathrm{lcm}(o,o')=oo'$ so that $b_0=\frac{\mathrm{lcm}(o,o')}{o}=o'$ and $a=0$ (because $\begin{pmatrix}0\\o'\end{pmatrix}$ is on the lattice): it's a rectangular lattice.

Resuming,

Conclusion

The minimum ordinate b_0 of an effective lattice L_x can be calculated directly from $\text{ord}(x)$ and $\text{ord}(1-x)$ ie from horizontal and vertical order of L_x.

Digress: the order of $1-x$

What can wee tell about the order of $1-x$?

First observation

The order of $1-x$ depends only of the minimal polynomial of x. More precisely: it is the order of $\Phi_x(1-X)$

Consequence

The orders of x and $1-x$ have the same degree.

For example it is not possible in $\mathbb{F}_3$ to have $\mathrm{ord}(x)=4$ and $\mathrm{ord}(1-x)=2$ because the order of 4 if 2 $(4|3^2-1)$ but the order of 2 is 1 $(2|3^1-1)$.

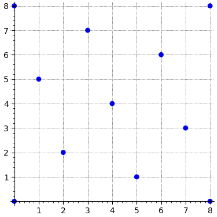
Note on $\mathrm{ord}(x)$ and $\mathrm{ord}(1-x)$

Second observation

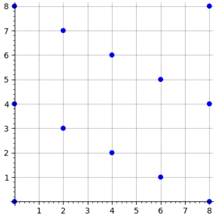
The order of $1-x$ doesn't only depend of $\mathrm{ord}(x)$.

For example: in $\mathbb{F}_3$

- With $\Phi_{8,1} = X^2 - X - 1$ we have $\Phi_{8,1}(1-X) = \ldots = \Phi_{8,1}(X)$ so that for any root x of $\Phi_{8,1}$ we have $\mathrm{ord}(x) = \mathrm{ord}(1-x) = 8$.
- With $\Phi_{8,2} = X^2 + X - 1$ we have $\Phi_{8,2}(1-X) = \ldots = \Phi_4(X)$ so that here $\mathrm{ord}(x) = 8$ but $\mathrm{ord}(1-x) = 4$.

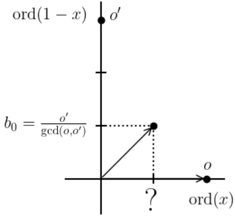


$L_{8,1} = L_{X^2-X-1}$



$L_{8,2} = L_{X^2+X-1}$

Step 2: abscissa of minimum ordinate vector



Given an effective lattice L_x we have an unique basis $v_1 = \begin{pmatrix} o \\ 0 \end{pmatrix}$, $v_2 = \begin{pmatrix} a \\ b_0 \end{pmatrix}$ with b_0 the minimal ordinate of the lattice and $0 \leq a < o$.

We have seen how to find b_0 from $o = \operatorname{ord}(x)$ and $o' = \operatorname{ord}(1-x)$

$$b_0 = \frac{\operatorname{lcm}(o,o')}{o'} = \frac{o'}{\gcd(o,o')}$$

The question is now: how to find a?

Step 2: miscellaneous observations

- First observation: we can reasonate on L_{1-x} (symetric of L_x) to show that the minimal abscissa a_0 is

$$a_0 = \frac{o}{\gcd(o, o')}$$

As a result a is a multiple of $\frac{o}{\gcd(o,o')}$.

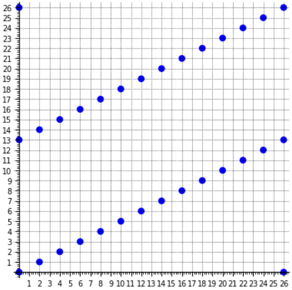
- Second observation: as $x^a(1-x)^{b_0} - 1 = 0$ ie $X^a(1-X)^{b_0} - 1 = 0$ in $\mathbb{F}_q = \mathbb{F}_p[X]/(\phi(X))$ (where we note ϕ for the minimum polynomial of x) as $\deg(\phi) = f$ and $\phi | X^a(1-X)^{b_0} - 1$ then $f \leq a + b_0$ so $a \geq f - b_0$.
- Third observation: as $x^o = 1$ then we can get $a < o$

Basic constrains on a

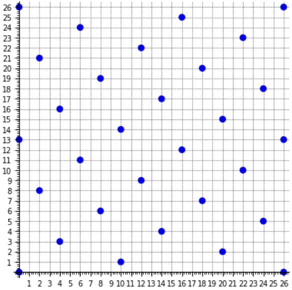
The number a is a multiple of $\frac{o}{\gcd(o,o')}$ and $f - b_0 \leq a < o$.

Step 2: last observation

Last observation observation: contrarily to b_0, we can't calculate a directly from o and o' as the following lattices in $\mathbb{F}_3$ show:



$L_{26,1} = L_{x^3-x^2+1}$



$L_{26,2} = L_{x^3-x+1}$

Step 2: let's set the frame

⚠Change of letter: the lattices of order o are lattices of the form L_z where $z \in \mathbb{F}_{p^f}$ where f is the degree of the minimal polynomial of z.
Let $\mathbb{F}_{p^f} = \mathbb{F}_p[X]/(P)$ where P is a **primitive** irreducible polynomial ie $x = X \mod P$ generates the cyclic group $\mathbb{F}^*_{p^f}$.
In other words the map $\alpha \mapsto x^\alpha$ gives an isomorphism $\mathbb{Z}_{p^f-1} \xrightarrow{\sim} \mathbb{F}^*_{p^f}$.
Its inverse will be noted $\log_x : \mathbb{F}^*_{p^f} \xrightarrow{\sim} \mathbb{Z}_{p^f-1}$.

Step 2: switching to $\mathbb{Z}_{p^f-1}$

We can now traduce the problem in $\mathbb{Z}_{p^f-1}$: if $z = x^\alpha$,

$$\begin{aligned} z^a(1-z)^b = 1 &\iff a\log_x(z) + b\log_x(1-z) \equiv 0 \bmod p^f - 1 \\ &\iff a\alpha + b\log_x(1-x^\alpha) \equiv 0 \mod p^f - 1 \end{aligned}$$

Here the number $b = b_0$ being known, the only unknown is a.

To solve

Find a in $\mathbb{Z}_{p^f-1}$ such that $a\alpha + b_0\log_x(1-x^\alpha) \equiv 0$

Step 2: the key function ψ

A remark: we see here that all depend on the map

$$\alpha \mapsto \alpha' = \psi(\alpha) = \log_x(1 - x^{\alpha})$$

This map is the traduction of $z \mapsto 1 - z$ in $\mathbb{F}_{p^f}^* = \mathbb{Z}_{p^f-1}$:

$$\begin{tikzcd}
\mathbb{Z}_{p^f-1} \arrow[r, "\psi"] \arrow[d, "\wr"'] & \mathbb{Z}_{p^f-1} \arrow[d, "\wr"'] \\
\mathbb{F}_{p^f}^* \arrow[r, "1-x"] & \mathbb{F}_{p^f}^*
\end{tikzcd}$$

Step 2: solving the problem in $\mathbb{Z}_{p^f-1}$

Returning to our problem: find $a \in \mathbb{Z}_{p^f-1}$

$$\begin{aligned} z^a(1-z)^{b_0} = 1 &\iff a\log_x(z) + b_0\log_x(1-z) \equiv 0 \\ &\iff a\alpha + b_0\log_x(1-x^\alpha) \equiv 0 \\ &\iff a\alpha + b_0\psi(\alpha) \equiv 0 \mod p^f - 1 \end{aligned}$$

Finding a is in fact equivalent to solve a Bezout equation of unknown a and q:

$$a\alpha + q(p^f - 1) = -b_0\psi(\alpha)$$

Hence the map ψ permits to abstract us from the field structure (it put it in a black box) and stay in the cyclic group $\mathbb{Z}_{p^f-1}$ where the equation $X^a(1-X)^b = 1$ is not else but a Bezout equation.

Algorithm to find all lattice of order o

1. Calculate the degree f of o: $f = \mathrm{ord}_o(p)$
2. Find all elements of order o in $\mathbb{Z}_{p^f-1}$ (to be precise we must find a list a elements not conjugate in $\mathbb{F}_{p^f}$)
3. For each element α of the list, calculate $\alpha' = \phi(\alpha)$.
4. Calculate $o' = \mathrm{ord}(\alpha')$ and $b_0 = \frac{o'}{gcd(o,o')}$.
5. Find with Bezout the smallest positive a such that

$$a\alpha + q(p^f - 1) = -b_0\alpha'$$

Factorisation with the lattices

We have found all the lattices of given order o, so all the lattices of given degree f by considering all order of given degree f.

This gives tables of all possible lattices.

We will see now how uses theses tables to factor "by hand" the polynomials $X^u(1-X)^v-1$.

Factorisation with lattices: using the table

- Given $\mu_{u,v} = X^u(1-X)^v - 1$, we know that the degree of factors of $\mu_{u,v}$ is less than $u+v$ so that its order must divide a $p^f - 1$ with $f \leq u+v$:
  a priori we must have the database of all lattices of orders dividing the $p^f - 1$ for $f \leq u+v$.
  (We will see that we can a little reduce this table but it will stay big)
- For each possible $f \leq u+v$ and for each effective lattice L of degree f we must check if $(u,v) \in L$.
- Remark: we can easily show $\mu_{u,v}$ has factors with power only if $(u+v)^{u+v} = u^u v^v$ in $\mathbb{F}_p$ and in this case there is a square linera factor $X - \frac{u}{u+v}$. We can so easily count the total degree of the factors and know when $\mu_{u,v}$ is totally factorised without always go through $f = u+v$.

Presentation of the tables

For each degree f we give a table

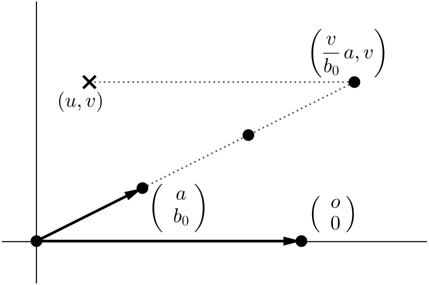
$b_0 \backslash a_0$	1	…
1	$((o,0),(a,b_0))$ $((o',0),(a',b'_0))$	…
…	…	…

The table needn't contain all a_0 and b_0 for a given (u,v) because for (u,v) to be in the lattice $\mathbb{Z}\begin{pmatrix} o \\ 0 \end{pmatrix} + \mathbb{Z}\begin{pmatrix} a \\ b_0 \end{pmatrix}$ we must have $b_0|v$ and for symetric reason $a_0|u$.

A remark: our table above do not mention the irreducible factor. We could track this in the table by computing the minimal polynomials, but we are mainly interested in the repartition of degrees and orders.

Verify the belonging of a lattice

For each (a_0, b_0) such that $a_0|u$ and $b_0|v$ we have to verify if (u, v) is in on of the lattice of the cell.
The following figure show that it is in a given lattice $((o,0),(a,b_0))$ if and only if $o|\frac{v}{b_0}a-u$.



An example

We want modulo 3 to factor the polynomial $\mu_{2,3} = X^2(1-X)^3 - 1$.
We first verify if $(u+v)^{u+v} = u^u v^v$ to know if there is ramification: no, because here $v^v = 0$.
We consider first the degree 1 factors given by the following table:

	1
1	((2, 0), (1, 1))

$$3\begin{pmatrix}1\\1\end{pmatrix} - \begin{pmatrix}2\\3\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} \notin \begin{pmatrix}2\\0\end{pmatrix}\mathbb{Z}$$

An example: degree 2

Then for the degree 2:

	1	2
1	((8, 0), (5, 1))	((8, 0), (6, 1))
2	((4, 0), (3, 2))	

There are two lattices to consider:

- Lattice $((8,0),(5,1))$:
  $3\begin{pmatrix}5\\1\end{pmatrix} - \begin{pmatrix}2\\3\end{pmatrix} = \begin{pmatrix}13\\0\end{pmatrix} \notin \begin{pmatrix}8\\0\end{pmatrix}\mathbb{Z}$
- Lattice $((8,0),(6,1))$:
  $3\begin{pmatrix}6\\1\end{pmatrix} - \begin{pmatrix}2\\3\end{pmatrix} = \begin{pmatrix}16\\0\end{pmatrix} \in \begin{pmatrix}8\\0\end{pmatrix}\mathbb{Z}$
- We do not consider the lattice $((4,0),(3,2))$ because here $b_0 = 2 \nmid 3$

An example: degree 3

As we found a degree 2 factor there is only one degree 3 factor left to find. The following table show the possible degree 3 effective lattices with a_0 and b_0 lower than 10.

	1	2
1	((13, 0), (8, 1)) ((13, 0), (5, 1)) ((26, 0), (9, 1)) ((26, 0), (3, 1))	((26, 0), (10, 1)) ((26, 0), (2, 1))
2	((13, 0), (1, 2)) ((13, 0), (8, 2))	

- Lattice $((13,0),(8,1))$:
  $$3\begin{pmatrix}8\\1\end{pmatrix}-\begin{pmatrix}2\\3\end{pmatrix}=\begin{pmatrix}22\\0\end{pmatrix}\notin\begin{pmatrix}13\\0\end{pmatrix}\mathbb{Z}$$
- Lattice $((13,0),(5,1))$:
  $$3\begin{pmatrix}5\\1\end{pmatrix}-\begin{pmatrix}2\\3\end{pmatrix}=\begin{pmatrix}13\\0\end{pmatrix}\in\begin{pmatrix}13\\0\end{pmatrix}\mathbb{Z}$$

An example: conclusion

Conclusion: the polynomial $\mu_{2,3} = X^2(1-X)^3 - 1$ has two factors, one factor of degree 2 and order 8, and a factor of degree 3 and order 13.