On Polynomial Modular Number Systems over Z/pZ

Jean-Claude Bajard, Jérémy Marrez, Thomas Plantard, Pascal Véron

On Polynomial Modular Number Systems over $\mathbb{Z}/p\mathbb{Z}$

Jean Claude Bajard[a], Jérémy Marrez[b], Thomas Plantard[c], Pascal Véron[d]

[a] *Sorbonne Université, CNRS, Inria, Institut de Mathématiques de Jussieu – Paris Rive Gauche, France*
[b] *Sorbonne Université, CNRS, Laboratoire d'informatique de Paris 6, Paris, France*
[c] *University of Wollongong, Institute of Cybersecurity and Cryptology, Wollongong, Australia*
[d] *Université de Toulon, Institut de Mathématiques, Toulon, France*

Abstract

Polynomial Modular Number System (PMNS) is a convenient number system for modular arithmetic, introduced in 2004. The main motivation was to accelerate arithmetic modulo an integer p. An existence theorem of PMNS with specific properties was given. The construction of such systems relies on sparse polynomials whose roots modulo p can be chosen as radices of this kind of positional representation. However, the choice of those polynomials and the research of their roots are not trivial.

In this paper, we introduce a general theorem on the existence of PMNS and we provide bounds on the size of the digits used to represent an integer modulo p.

Then, we present classes of suitable polynomials to obtain systems with an efficient arithmetic. Finally, given a prime p, we evaluate the number of roots of polynomials modulo p in order to give a number of PMNS bases we can reach. Hence, for a fixed prime p, it is possible to get numerous PMNS, which can be used efficiently for different applications based on large prime finite fields, such as those we find in cryptography, like RSA, Diffie-Hellmann key exchange and ECC (Elliptic Curve Cryptography).

Keywords: Polynomial Modular Number System, Polynomial roots, Finite field, Modular Computation

Introduction

∗. jean-claude.bajard@sorbonne-universite.fr

Email addresses: jean-claude.bajard@sorbonne-universite.fr (Jean Claude Bajard), jeremy.marrez@sorbonne-universite.fr (Jérémy Marrez), thomaspl@uow.edu.au (Thomas Plantard), pascal.veron@univ-tln.fr (Pascal Véron)

Polynomial Modular Number System (PMNS) was introduced in 2004 [20] as a representation system that allows implementation of an effective modular arithmetic involving only additions and multiplications. Arithmetic operations called modular addition, modular multiplication and modular reduction occur in several of today's public key cryptography algorithms such as the well-known RSA, Diffie-Hellman key exchange and ECC [15]. These computations modulo an integer p consist in adding or multiplying two integers, then recovering the remainder modulo p. The way to perform those operations varies depending on the form of p (for example Mersenne numbers, of the form $2^m - 1$ allow fast reduction). PMNS offers both the advantages of fast polynomial arithmetic and easy parallelization for an arbitrary p, with algorithms more efficient than known division free methods such as Montgomery [18] or Barrett[4].

The main idea behind the PMNS is that it is a modular system, where integers modulo an arbitrary p (not necessarily prime) are represented by polynomials of degree smaller than a fixed integer n. The coefficients of the polynomials are the digits and are bounded by an integer ρ, which is small relatively to p ($\rho \simeq p^{1/n}$). Construction of such systems is based on sparse polynomials whose roots γ are used as the radices of this kind of positional representation. The interest of these sparse polynomials lies in the efficiency of the modular arithmetic spawned. Those operations are done in two steps. First, the operations are carried out on polynomials modulo a sparse polynomial $E(X)$, called polynomial reduction, which is of degree n, and this reduction ensures that the degree of the result is smaller than n. Then, a coefficient reduction is performed involving the Euclidean lattice associated with the system [11, 21, 10], guaranteeing that the coefficients of the result are bounded by ρ. The number of PMNS systems that we can generate from an integer p is directly related to the number of roots of the reduction polynomial $E(X)$ in $\mathbb{Z}/p\mathbb{Z}$.

A method for constructing an efficient PMNS was published in 2004 [3]. The system is built from two sparse polynomials with good reduction properties (one for polynomial reduction, $E(X)$, one for coefficient reduction), in order to derive the integer p through the calculation of a resultant, and also one root γ. We keep only cases where p is prime, since p is likely to be prime for practical cryptographic applications such as Diffie-Hellman and ECC. However, for most cryptographic protocols, the modulo p used is often fixed or at least has strong mathematical properties required. Hence, in order to be able to work with arbitrary p, prime or not, a theorem [2] gives a construction of PMNS from an integer p, a number of digits n and an integer polynomial $E(X)$ of the form $E(X) = X^n + aX + b$ satisfying some assumptions. Thus, this theorem guarantees the existence of the PMNS system $\mathfrak{B} = (p, n, \gamma, \rho)_E$, with a bound on ρ. Nevertheless, building such systems from a given p is not trivial. To obtain an example of a PMNS system from a fixed p, one has to seek a sparse polynomial $E(X)$ satisfying the conditions of the theorem, and one of its roots in $\mathbb{Z}/p\mathbb{Z}$. Very recently, the use of PMNS to perform modular multiplications was reintroduced in [12], where we find some interesting complexity theoretical bounds.

In this paper, given a number p, we want to provide as many PMNS bases as possible with efficient reduction polynomials. Therefore, we propose, in section 1, a theorem which gives, as criterium of existence, a bound on the digits size in function of any polynomial $E(X)$, and some properties when $E(X)$ is irreducible. Then, in section 3, we propose classes of suitable irreducible polynomials that satisfy the previous theorems, allowing efficient reductions, and whose roots can be clearly identified in a finite prime field $\mathbb{Z}/p\mathbb{Z}$. In Section 4, we gives the number of roots in function of p and the reduction polynomial $E(X)$. Those roots are used to generate the Euclidean lattice associated with the system, and act directly on the coefficient reduction, making this search an important challenge to obtain efficient representations in terms of calculation and storage. Thus, for a given prime number p, it is now possible to obtain many PMNS bases with their own computational properties. This ability to provide several equivalent representations is also an interesting point in terms of performance if we want to mask the computations to protect an implantation against malicious observers.

1. Polynomial Modular Number System

We recall the definition of *a classical positional number system.* For a given integer β greater or equal than 2, β is called the radix or the base, an integer $a \in \mathbb{N}$ with $a < \beta^m$ can be represented by an unique sequence of integers $(a_i)_{i=0\ldots m-1}$, called digits, such that $a = \sum_{i=0}^{m-1} a_i\beta^i$, with $a_i \in \mathbb{N}$, $0 \leq a_i < \beta$.

Let $p \in \mathbb{N}$, $\beta^{n-1} \leq p < \beta^n$, $\beta^n \equiv \delta \pmod{p}$, the following algorithm returns $c < \beta^n$ with $a \equiv c \pmod{p}$:

```
       $c \leftarrow a$
  do
      1. $c \rightarrow c_0 + \beta^n c_1$ with $c_0, c_1 < \beta^n$
      2. $c \leftarrow c_0 + \delta c_1$
  until $c < \beta^n$,
return $a \equiv c \pmod{p}$,
```

If $\delta \leq \beta^{\mathbf{\frac{1}{2}n}}$ then two iterations gives $a < 2\beta^n - \beta^{\frac{1}{2}n} - 1$, if necessary, a last subtraction gives $a < \beta^n$.

For our purpose, this reduction can be decomposed using a polynomial approach. Since, $\beta^n - \delta \equiv 0 \pmod{p}$, then β can be considered as a root modulo p of the polynomial $E(X) = X^n - \Delta(X)$ where $\Delta(\beta) \equiv \delta \pmod{p}$.

Thus the reduction modulo p is computed with the iterations split in two steps :

1. polynomial reduction : $C(X) = A(X) \bmod E(X)$
2. coefficients reduction : $C'(\beta) \equiv C(\beta) \pmod{p}$ with $C'(X)$ of degree $n-1$ and coefficients smaller than β

The polynomial reduction should be a fast rough reduction of the size (the degree), then the coefficient reduction reduces the coefficients to digit values smaller than β. Typically, the polynomial reduction looks like :

1. $C(X) = A(X)$
2. do until degree of $C(X)$ lower than n, (the degree decreases about $(n-t)$)
   $C(X) = \Delta(X) \times \sum_{i=n}^{m-1} c_i X^{i-n} + \sum_{i=0}^{n-1} c_i X^i$

Thus, if t the degree of $\Delta(X)$ is lower than $n/2$ and $m < 2n$, then at the first step of the loop $\deg C(X) = t+m-n-1$ and after the second one $\deg C(X) < n-1$. Now, if $\Delta(X)$ is sparse with small coefficients then the multiplication by $\Delta(X)$ corresponds to few shifts and additions only [22].

Unfortunately, it is not obvious to find a couple $\beta, E(X)$ with good features, in classical positional number systems. To get more opportunity of such couple, a new kind of representation was introduced in [2], where the base, for a given p, deeply depends of the choice of the reduction polynomial $E(X)$.

Definition 1.1. A *Polynomial Modular Number System* (PMNS) is defined by a quadruple (p, n, γ, ρ) and a polynomial $E \in \mathbb{Z}[X]$, called *reduction polynomial* with respect to p, such that for each integer x in $\{0, \dots p-1\}$, there exists $(x_0, \dots, x_{n-1})$ with $x \equiv \sum_{i=0}^{n-1} x_i \gamma^i \pmod{p}$, where $x_i \in \mathbb{N}$, $-\rho < x_i < \rho$, $0 < \gamma < p$, and $E(\gamma) \equiv 0 \pmod{p}$, with $E(X)$ a monic polynomial of degree n.

Example 1.1. Let us consider two PMNS defined as $\mathfrak{B} = (p, n, \gamma, \rho)_E$.

A first, with $p = 23$, $n = 3$, $\gamma = 7$ and $\rho = 2$, for representing the elements of $\mathbb{Z}/23\mathbb{Z}$ as vectors with 4 digits belonging to { -1, 0, 1}. We note that $\gamma^3 + 2 \equiv 0 \bmod 23$ (i.e. $E(X) = X^3 + 2$).

0	1	2	3	4	5	6	7
(0, 0, 0)	(1, 0, 0)	(-1, 0, 1)	(-1, 1, -1) (0, 0, 1)	(0, 1, -1) (1, 0, 1)	(1, 1, -1)	(-1, 1, 0)	(0, 1, 0)
8	9	10	11	12	13	14	15
(1, 1, 0)	(-1, 1, 1)	(0, 1, 1)	(1, 1, 1)	(-1,-1,-1)	(0, -1, -1)	(1, -1, -1)	(-1, -1, 0)
16	17	18	19	20	21	22	
(0, -1, 0)	(1, -1, 0)	(-1, -1, 1)	(-1, 0, -1) (0, -1, 1)	(0, 0, -1) (1, -1, 1)	(1, 0, -1)	(-1, 0, 0)	

Now with $p = 31$, $n = 4$, $\gamma = 15$ and $\rho = 2$, for representing the elements of $\mathbb{Z}/31\mathbb{Z}$ as vectors with 3 digits belonging to { -1, 0, 1}. We note that $\gamma^4 - 2 \equiv 0 \bmod 31$.

0	1	2	3	4	5
(0, 0, 0, 0)	(1, 0, 0, 0)	(-1, 1, -1, 1)	(-1, -1, -1, 1) (-1, 0, 0, -1) (-1, 0, 1, 1) (0, 1, -1, 1)	(0, -1, -1, 1) (0, 0, 0, -1) (0, 0, 1, 1) (1, 1, -1, 1)	(1, -1, -1, 1) (1, 0, 0, -1) (1, 0, 1, 1)
6	7	8	9	10	11
(-1, 1, -1, 0)	(-1, -1, -1, 0) (-1, 0, 1, 0) (0, 1, -1, 0)	(0, -1, -1, 0) (0, 0, 1, 0) (1, 1, -1, 0)	(1, -1, -1, 0) (1, 0, 1, 0)	(-1, 1, -1, -1) (-1, 1, 0, 1)	(-1, -1, -1, -1) (-1, -1, 0, 1) (-1, 0, 1, -1) (0, 1, -1, -1) (0, 1, 0, 1)
12	13	14	15	16	17
(0, -1, -1, -1) (0, -1, 0, 1) (0, 0, 1, -1) (1, 1, -1, -1) (1, 1, 0, 1)	(1, -1, -1, -1) (1, -1, 0, 1) (1, 0, 1, -1)	(-1, 1, 0, 0)	(-1, -1, 0, 0) (0, 1, 0, 0)	(0, -1, 0, 0) (1, 1, 0, 0)	(1, -1, 0, 0)
18	19	20	21	22	23
(-1, 0, -1, 1) (-1, 1, 0, -1) (-1, 1, 1, 1)	(-1, -1, 0, -1) (-1, -1, 1, 1) (0, 0, -1, 1) (0, 1, 0, -1) (0, 1, 1, 1)	(0, -1, 0, -1) (0, -1, 1, 1) (1, 0, -1, 1) (1, 1, 0, -1) (1, 1, 1, 1)	(1, -1, 0, -1) (1, -1, 1, 1)	(-1, 0, -1, 0) (-1, 1, 1, 0)	(-1, -1, 1, 0) (0, 0, -1, 0) (0, 1, 1, 0)
24	25	26	27	28	29
(0, -1, 1, 0) (1, 0, -1, 0) (1, 1, 1, 0)	(1, -1, 1, 0)	(-1, 0, -1, -1) (-1, 0, 0, 1) (-1, 1, 1, -1)	(-1, -1, 1, -1) (0, 0, -1, -1) (0, 0, 0, 1) (0, 1, 1, -1)	(0, -1, 1, -1) (1, 0, -1, -1) (1, 0, 0, 1) (1, 1, 1, -1)	(1, -1, 1, -1)
30					
(-1, 0, 0, 0)					

We can remark that the redundancy depends of the number of digits $2\rho - 1$, the degree n and the modulo p. The redundancy is not equidistributed but we can see a symmetry due to the sign of the value modulo p.

Proposition 1.1. *If $\mathfrak{B} = (p, n, \gamma, \rho)_E$ is a PMNS, then $p \leq (2\rho - 1)^n$.*

Proof. The number of representations in $\mathfrak{B}$ is $(2\rho - 1)^n$, this number must be at least greater than p, i.e. the number of values $0 \leq x < p$. □

Remark.

1. PMNS looks like a positional system, but $(\gamma^i \bmod p) < (\gamma^{i+1} \bmod p)$ is not always true anymore.

2. For every quadruple (p, n, γ, ρ), there exists a polynomial $E(X) \in \mathbb{Z}[X]$ satisfying $E(\gamma) \equiv 0 \mod p$ and $\deg E(X) = n$:
for example $E(X) = X^n - (\gamma^n \mod p)$.
3. If $p < (2\rho - 1)^n$, then the representation is redundant (i.e., some values can have more than one representation).
4. If $\mathfrak{B} = (p, n, \gamma, \rho)_E$ is a PMNS, so is $\mathfrak{B}' = (p, n, \gamma, \rho + 1)_E$.
Given p, n, γ, in order to minimize the redundancy of the system, it could be judicious to take ρ as the smallest integer such that (p, n, γ, ρ) is a PMNS. We denote ρ_{min} this integer. ρ_{min} can be determined with a lattice reduction [20], it gives the minimal representation size for a given n.

The question, for p and n given. Which polynomials $E(X)$

-i) offer a good modular reduction,

-ii) have a large number of roots γ in $\mathbb{Z}/p\mathbb{Z}$,

-iii) allow to have ρ as small as possible, to ensure several PMNS, both compact and with an efficient arithmetic on representations ?

Notations. In the following, we note $A(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$ the polynomial and $A = (a_0, a_1, \ldots, a_{n-1})$ the corresponding vector. We will use this different notations in function of the purpose.

2. Theorem of bounds and existence of a PMNS

In this section, we give conditions to ensure the existence of a PMNS $\mathfrak{B} = (p, n, \gamma, \rho)_E$.

2.1. Lattice associated to a PMNS

We consider the lattice $\mathfrak{L}$ over $\mathbb{Z}^n$ of the polynomials of degree at most $n - 1$, for which, γ is a root modulo p (see [16] for basics on lattices theory) .

We define this lattice by giving $\mathbf{A}$, one of its bases, whose elements are $A_0 = (p, 0, \ldots, \ldots, 0)$ (i.e., $A_0(X) = p$), and $A_i = (0, \ldots, -\gamma, 1_i, \ldots, 0)$ (i.e. $A_i(X) = X^i - \gamma X^{i-1}$), for $1 \leq i \leq n - 1$. Thus with A_0 all the multiples of p have a representation in this lattice, and the A_i for $0 \leq i \leq n-1$ are linearly independent. The fundamental volume of $\mathfrak{L}$ is $\det \mathbf{A} = p$.

Remark. It is possible to consider $A'_i(X) = X^i - \gamma^i$, for $1 \leq i \leq n - 1$, which represents the same lattice $\mathfrak{L}$. We have $A_1(X) = A'_1(X) = X - \gamma$ and $A_i(X) = A'_i(X) - \gamma A'_{i-1}(X)$.

$$\mathbf{A} = \begin{pmatrix} p & 0 & \dots & \dots & 0 & 0 \\ -\gamma & 1 & \dots & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & & & \vdots \\ 0 & \dots & -\gamma & 1 & \dots & 0 \\ \vdots & & & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \dots & -\gamma & 1 \end{pmatrix}, \mathbf{A}' = \begin{pmatrix} p & 0 & 0 & \dots & 0 & 0 \\ -\gamma & 1 & 0 & \dots & 0 & 0 \\ \vdots & & \ddots & & & \vdots \\ -\gamma^i & \dots & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \ddots & \vdots \\ -\gamma^{n-1} & 0 & \dots & \dots & 0 & 1 \end{pmatrix} \quad (1)$$

Theorem 2.1. *Let $p \geq 2$ and $n \geq 2$ two integers, $E(X)$ a polynomial of degree n in $\mathbb{Z}[X]$ and γ be a root of $E(X)$ in $\mathbb{Z}/p\mathbb{Z}$.*
Let r be the covering radius of the lattice $\mathfrak{L}$, if $\rho > r$, then $\mathfrak{B} = (p, n, \gamma, \rho)_E$ is a Polynomial Modular Number System.

Proof. The covering radius r of $\mathfrak{L}$ is the smallest number, such that the balls $\mathcal{B}_V = \{T \in \mathbb{R}^n, \|T - V\|_2 \leq r\}$ centered on any point $V \in \mathfrak{L}$, cover the space $\mathbb{R}^n$. In other words, for any $T \in \mathbb{R}^n$ there exists $V \in \mathfrak{L}$ such that $\|T - V\|_\infty \leq \|T - V\|_2 \leq r$. Thus for any $T \in \mathbb{R}^n$ there exists $V \in \mathfrak{L}$, such that $T - V \in \mathcal{C}_O$, $\mathcal{C}_O = \{T \in \mathbb{R}^n, \|T\|_\infty \leq r\}$.

□

Remark. Let λ_n be the smallest integer such that $\mathfrak{L}$ contains at most n linearly independent vectors of length lower or equal to λ_n for the euclidien norm. A classical result of lattice theory states that the covering radius r, is such that, $\frac{1}{2}\lambda_n \leq r \leq \sqrt{n}\lambda_n$ [16].

An interpretation of Theorem 2.1. Let $a \in \mathbb{N}$ and let $F_a(X)$ be a polynomial such that $F_a(\gamma) \equiv a \bmod p$, then $T_a(X) = F_a(X) \pmod{E(X)}$, satisfies $T_a(\gamma) \equiv a \bmod p$ with $\deg T_a < n$ (polynomial reduction step).

Next, there exists $V \in \mathfrak{L}$ such that, $\|T_a - V\|_\infty < \rho$, and $(T_a - V)(\gamma) \equiv T_a(\gamma) - V(\gamma) \equiv a \bmod p$. Hence $T_a - V$ is a representative of a in the PMNS $\mathfrak{B}$. Therefore, any $a \in \mathbb{N}$ can be represented in the PMNS modulo p.

2.2. Lattice's bases and PMNS

Currently, to our knowledge, there is no efficient algorithm to compute the covering radius of a lattice. In this section, we provide a bound on ρ which can be computed from a base of a lattice $\mathfrak{L}$ defined by a matrix A.

Let $\mathrm{B} = \{B_0, \dots, B_{n-1}\}$ a base of $\mathfrak{L}$, and $\mathbf{B}$ the matrix associated such that, B_i represents the i^{th} row., with $B_i = (b_{i,0}, \dots, b_{i,n-1})$, thus $b_{i,j}$ represents the coefficient of the ith row, j^{th} column (number beginning by 0).

Theorem 2.2. *If* $\rho > \frac{1}{2}\left\|\mathbf{B}\right\|_1$*, (*$\left\|\mathbf{B}\right\|_1 = \max\limits_{j}\left\{\sum\limits_{i=0}^{n-1}|b_{i,j}|\right\}$*), then* $\mathfrak{B} = (p, n, \gamma, \rho)_E$ *is a Polynomial Modular Number System.*

Proof. Let $S \in \mathbb{R}^n$, we define :

- $\lfloor S \rceil$ as the vector whose coordinates are integers equal to the round to nearest of those of S.
- frac(S) as the vector $(S) = S - \lfloor S \rceil$, notice that $\|\text{frac}(S)\|_\infty \leq \frac{1}{2}$

Let $S \in \mathbb{R}^n$, we search a close vector $T \in \mathfrak{L}$ using a Babaï round-off approach [1]. We have, $T = \mathbf{B}^T.\lfloor(\mathbf{B}^T)^{-1}.S\rceil$.

$$S = \mathbf{B}^T.(\mathbf{B}^T)^{-1}.S = T + \mathbf{B}^T.\text{frac}\left((\mathbf{B}^T)^{-1}.S\right) \text{ with } \left\|\text{frac}\left((\mathbf{B}^T)^{-1}.S\right)\right\|_\infty \leq \frac{1}{2}$$

Then

$$\|S - T\|_\infty = \left\|\mathbf{B}^T.\text{frac}\left((\mathbf{B}^T)^{-1}.S\right)\right\|_\infty \leq \frac{1}{2}\left\|\mathbf{B}^T\right\|_\infty = \frac{1}{2}\left\|\mathbf{B}\right\|_1.$$

□

Remark. In order to minimize $\|\mathbf{B}\|_1$, a first general strategy is to compute a reduced base B of $\mathfrak{L}$ defined by $\mathbf{A}$ using algorithms like LLL, BKZ or HKZ [13].

The next strategies can be applied when the polynomial $E(X)$ is irreducible.

2.3. Irreducible polynomials and PMNS

Let $E(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, and let $\mathbf{C}$ be the companion matrix of $E(X)$:

$$\mathbf{C} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-2} & -a_{n-1} \end{pmatrix}.$$

Let $V = (v_0, \dots, v_{n-1})$ the vector representing the coefficient of the polynomial $V(X) = \sum_{i=0}^{n-1} v_iX^i$, then $V.\mathbf{C}$ is the vector whose coordinates are the coefficients of the polynomial $X.V(X)$ mod $E(X)$.

Proposition 2.3. *Let* V *a non-null vector of* $\mathfrak{L}$*, the lattice of rank* n *defined by* $\mathbf{A}$*, Equ. (1). Let* $B_i = V.\mathbf{C}^i$ *the row vector whose coordinates are the coefficients of the polynomial* $B_i(X) = X^i.V(X) \bmod E(X)$*. Let* $\mathbf{B}$ *the* $n \times n$ *matrix whose* i^{th} *row is the vector* B_i*.*

If $V(X)$ *is inversible modulo* $E(X)$ *then :*

— *the matrix* $\mathbf{B}$ *defines a sublattice* $\mathfrak{L}' \subseteq \mathfrak{L}$ *of rank* n *(i.e.* $\mathrm{B} = (B_0, \ldots, B_{n-1})$ *is a base of* $\mathfrak{L}'$*),*

— *and* $V \in \mathfrak{L}'$*.*

Proof. The B_i are linearly independent. Indeed, let us suppose that there exists a non nul vector $(t_0, t_1, \ldots, t_{n-1}) \in \mathbb{Z}^n$ such that $\sum_{i=0}^{n-1} t_i B_i = 0$. It means that $\sum_{i=0}^{n-1} t_i X^i V(X) = 0 \bmod E(X)$, or equivalently $T(X)V(X) = 0 \bmod E(X)$, with $T(X) = \sum_{i=0}^{n-1} t_i X^i$. Then $T(X)V(X)V^{-1}(X) \bmod E(X) = T(X) = 0$, since $V(X)$ is inversible modulo $E(X)$ and degree of $T(X)$ is at most $n-1$. Hence the rows of $\mathbf{B}$ are a base of a sublattice $\mathfrak{L}' \subseteq \mathfrak{L}$ of rank n, and $V \in \mathfrak{L}'$. □

Corollary 2.1. *Let* V *a non-null vector of* $\mathfrak{L}$*, the lattice of rank* n *defined by* $\mathbf{A}$*, Equ. (1).*

If $E(X)$ *is irreducible, then*

— V *can define a sublattice* $\mathfrak{L}' \subseteq \mathfrak{L}$ *of rank* n*,*

— *and* $V \in \mathfrak{L}'$*.*

Proof. If $E(X)$ is irreducible, then $V(X)$ is inversible and Proposition 2.3 gives $\mathrm{B} = (B_0, \ldots, B_{n-1})$ a base of $\mathfrak{L}'$, $\mathfrak{L}' \subseteq \mathfrak{L}$ of rank n, and $V \in \mathfrak{L}'$. □

Hence, the second strategy involves taking a short vector $V \in \mathfrak{L}$, that is a vector which satisfies the Minkowski bound, $\|V\|_\infty \leq \alpha(p)^{1/n}$ with $\alpha \in]0, 1]$.

In the last strategy we propose another way to compute the base B of $\mathfrak{L}'$.

Corollary 2.2. *Let* $\mathfrak{L}$*, the lattice of rank* n *given by* $\mathbf{A}$ *(Equ. (1)), and let the lattice* $\mathfrak{L}_D$ *of rank* n *in* $\mathbb{Z}^{n^2}$ *defined by* $\mathbf{D} = (\mathbf{A}|\mathbf{A}.\mathbf{C}^1|\cdots|\mathbf{A}.\mathbf{C}^{n-1})$*, then for any* $\overline{V} = (V_0, V_1, ..., V_{n-1}) \in \mathfrak{L}_D$ *such that* $\overline{V} \neq (0)^{n^2}$ *:*

If $E(X)$ *is irreducible then :*

1. $V_0 \in \mathfrak{L}$*,*
2. $(V_0, V_1, ..., V_{n-1})$ *is a base of* $\mathfrak{L}' \subseteq \mathfrak{L}$*.*

Proof. V_0 is a linear combination of rows of $\mathbf{A}$, hence it belongs to $\mathfrak{L}$. Next, since $V_i = V_0.\mathbf{C}^i$, for all $i \geq 1$, then, due to Corollary 2.1, the vector $(V_0, V_1, ..., V_{n-1})$ is a base of a sublattice $\mathfrak{L}' \subseteq \mathfrak{L}$. □

Hence, the last strategy is to choose a short vector $(V_0, V_1, ..., V_{n-1})$ of $\mathfrak{L}_D$ and to build the base B of $\mathfrak{L}$ from V.

2.4. Some examples of PMNS

In these examples we give the value of $\|\mathbf{B}\|_1$ for each reduced base approach : LLL or BKZ or HKZ reduction of $\mathbf{A}$, or the one of Corollary 2.1, or Corollary 2.2. We remark that the two last approaches offer the best results for polynomials $E(X)$ with small coefficients. In section 4.4, we give experimental results with exhaustive searches.

Example 2.1.

$p = 112848483075082590657416923680536930196574208889254960005437791530871071177777$

$n = 8$, $E(X) = X^8 + X^2 + X + 1$,

$\gamma = 14916364465236885841418726559687117741451144740538386254842986662265545588774$

LLL :	$\|\mathbf{B}\|_1 = 16940155314$	BKZ :	$\|\mathbf{B}\|_1 = 15289909984$
HKZ :	$\|\mathbf{B}\|_1 = 15289909984$		
Cor. 2.1 :	$\|\mathbf{B}\|_1 = 13881325101$	Cor. 2.2, :	$\|\mathbf{B}\|_1 = 12883199915$

Example 2.2.

$p = 96777329138546418411606037850670691916278980249035796845487391462163262877831$

$n = 8$, $E(X) = X^8 - X^4 - 1$,

$\gamma = 66378119609141043317728290217053385256449145407556727004132373270146455575461$

LLL :	$\|\mathbf{B}\|_1 = 17955608045$	BKZ :	$\|\mathbf{B}\|_1 = 17955608045$
HKZ :	$\|\mathbf{B}\|_1 = 17955608045$		
Cor. 2.1 :	$\|\mathbf{B}\|_1 = 11628752571$	Cor. 2.2 :	$\|\mathbf{B}\|_1 = 10489321362$

Example 2.3.

$p = 94234089378179148303661339351342500658910595299680545500602453424882978290351$

$n = 8$, $E(X) = X^8 + X^4 - X^3 + 1$,

$\gamma = 55857489577292751855009098551500852039618350925837275620376166398325678525151$

LLL :	$\|\mathbf{B}\|_1 = 12305954812$	BKZ :	$\|\mathbf{B}\|_1 = 12305954812$
HKZ :	$\|\mathbf{B}\|_1 = 12305954812$		
Cor. 2.1 :	$\|\mathbf{B}\|_1 = 15570303402$	Cor. 2.2 :	$\|\mathbf{B}\|_1 = 14857375293$

Example 2.4.

$p = 96777329138546418411606037850670691916278980249035796845487391462163262877831$

$n = 8$, $E(X) = X^8 + 6$,

$\gamma = 5538274654329514802181726618906590237936295237553666062542808070676484572674$

LLL :	$\|\mathbf{B}\|_1 = 12509178620$	BKZ :	$\|\mathbf{B}\|_1 = 12509178620$
HKZ :	$\|\mathbf{B}\|_1 = 12509178620$		
Cor. 2.1 :	$\|\mathbf{B}\|_1 = 47611052126$	Cor. 2.2 :	$\|\mathbf{B}\|_1 = 40733847267$

3. Suitable irreducible polynomials for PMNS

In Theorem 2.1, we show that if $E(X)$ is an irreducible polynomial, then we can define a PMNS $\mathfrak{B} = (p, n, \gamma, \rho)_E$ depending of $E(X)$. Now, for an algorithmic purpose about the reduction modulo $E(X)$, with respect to the size of the digits in $\mathfrak{B} = (p, n, \gamma, \rho)_E$, $E(X)$ must respect some criteria. Thus we define what can be a suitable PMNS irreducible reduction polynomial.

3.1. Suitable PMNS reduction polynomial

Definition 3.1. A polynomial $E(X)$ is a suitable PMNS reduction polynomial, if :

1. $E(X)$ is irreducible in $\mathbb{Z}[X]$,
2. $E(X) = X^n + a_k X^k + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, with $n \geq 2$ and $k \leq \frac{n}{2}$,
3. most of coefficients a_i are zero, and others are very small (if possible equal to ± 1) compare to $p^{1/n}$.

The second item ensures that the polynomial reduction modulo $E(X)$ of a polynomial $T(X)$ of degree lower than $2n$, is done in two steps, i.e. $T(X) = T_1(X)X^n + T_0(X)$ with $T_1(X)$ and $T_0(X)$ of degree lower than n, and $X^n \bmod E(X) = -(\sum_{i=0}^{k} a_i X^i) \bmod E(X)$.

The third item allows to give a bound on the coefficients of $T(X) \bmod E(X)$, namely $\|T(X) \bmod E(X)\|_\infty < s\|T(X)\|_\infty$, where s is the 1−norm of the $(2n-1) \times n$ matrix S whose row i represents the coefficients of $X^i \pmod{E(X)}$ for $i = 0 \ldots 2n-1$ (see Prop. 2.3 of [7]). As a consequence, if $G(X)$ and $F(X)$ are two elements of the PMNS, i.e. $\|F(X)\|_\infty < \rho$ and $\|G(X)\|_\infty < \rho$ then $\|F(X) \times G(X)\|_\infty < n\rho^2$ and $\|F(X) \times G(X) \pmod{E(X)}\|_\infty < sn\rho^2$.

For the first item, we must find an irreducible polynomial. Then to be a suitable PMNS reduction polynomial $E(X)$ must satisfy the two other items. In the sequel, we adapt some classical irreducibility criteria and give example of irreducible polynomials with few non zero coefficients.

3.2. Classical polynomial irreducibility criteria

To verify the first item, we can use general criteria like Schönemann-Eisenstein or Dumas [8] or the generalization given by N. C. Bonciocat in [6], that we adapt to our purpose : a monic polynomial $E(X) = X^n + a_k X^k + \cdots + a_1 X + a_0$.

Proposition 3.1 (from Dumas' criterion [8]). *We assume that if there exists a prime μ and an integer α, such that, $\mu^\alpha \mid a_0$, $\mu^{\alpha+1} \nmid a_0$ and, $\mu^{\lceil \alpha(n-i)/n \rceil} \mid a_i$, and* $\gcd(\alpha, n) = 1$, *then $E(X) = X^n + a_k X^k + \cdots + a_1 X + a_0$ is irreducible over $\mathbb{Z}[X]$.*

For example, $E(X) = X^n + \mu X^k + \mu$ is irreducible with this criterion. If $k < n/2$ and $\mu << p^{1/n}$, then $E(X)$ is a suitable PMNS reduction polynomial.

Proposition 3.2 (from Corollary 1.2 [6]). *Let $E(X) = X^n + a_k X^k + \cdots + a_1 X + a_0$, $a_0 \neq 0$, let $t \geq 2$ and let $\mu_1, \ldots, \mu_t$ be pair-wise distinct numbers, and $\alpha_1, \ldots, \alpha_t$ positive integers. If, for $j = 1, \ldots, t$, and $i = 0, \ldots, k$, $\mu_j^{\alpha_j} \mid a_i$ and $\mu_j^{\alpha_j+1} \nmid a_0$, and* $\gcd(\alpha_1, \ldots, \alpha_t, n) = 1$ *then $E(X)$ is irreducible over $\mathbb{Z}[X]$.*

For example, $E(X) = X^n + \mu_1^{\alpha_1}\mu_2^{\alpha_2}X^k + \mu_1^{\alpha_1}\mu_2^{\alpha_2}$ with $\gcd(\alpha_1, \alpha_2, n) = 1$, is irreducible with this criterion. If $k < n/2$ and $\mu_1^{\alpha_1}\mu_2^{\alpha_2} << p^{1/n}$, then $E(X)$ is a suitable PMNS reduction polynomial.

3.3. Suitable Cyclotomic Polynomials for PMNS

A well known set of irreducible polynomials in $\mathbb{Z}[X]$ is the set of cyclotomic polynomials. Let us denote by $\texttt{ClassCyclo}(\texttt{n})$ the class of suitable cyclotomic polynomials for PMNS, whose degree is n.

Proposition 3.3. *$\texttt{ClassCyclo}(\texttt{n}) \neq \emptyset$ if and only if, $n = 2^i3^j$ with $i \geq 1, j \geq 0$.*

Proof. Let us first recall some classical properties on cyclotomic polynomials :

(a) Let $m \in \mathbb{N}^*$, the m^{th} cyclotomic polynomial is defined as :

$$\Phi_m(X) = \prod_{\substack{k=1\\ \gcd(k,m)=1}}^{m} (X - \zeta^k)$$

with ζ a primitive m^{th} root of unity, $\deg \Phi_m(X) = \varphi(m)$ (φ is Euler's totient function) and $\Phi_m(X)$ is a monic polynomial, i.e. $a_{\varphi(m)} = 1$.

(b) Let $m > 1$ and let $n = \varphi(m)$, $\Phi_m(X)$ is self-reciprocal, $\Phi_m(X) = X^n\Phi_m(\frac{1}{X})$ (we can prove that they have the same roots), i.e. $a_i = a_{n-i}$.

(c) Let $m = \prod_{i=1}^r p_i^{e_i}$ and $m_0 = \prod_{i=1}^r p_i$, then $\Phi_m(X) = \Phi_{m_0}(X^{m/m_0})$.

(d) Let $m = 2t$ with t odd and $t \geq 3$ then $\Phi_m(X) = \Phi_t(-X)$.

Let n such that $\texttt{ClassCyclo}(\texttt{n}) \neq \emptyset$, hence there exists an integer m such that $n = \varphi(m)$ and $\Phi_m(X)$ is a suitable cyclotomic reduction polynomial. From (b), it means that $\Phi_m(X)$ is either $X^n + 1$ or $X^n + a_{n/2}X^{n/2} + 1$. Hence $\Phi_m(X)$ has 2 or 3 coefficients.

Let $m = \prod_{i=1}^r p_i^{e_i}$, $e_i \geq 0, p_1 = 2, p_2 = 3\ldots$ and $m_0 = \prod_{\substack{i=1\\ e_i\neq 0}}^{r} p_i$. From (c), if $e_1 = 0$ then $\Phi_m(X) = \Phi_{m_0}(X^{m/m_0})$. If $e_1 \neq 0$, from (c) and (d), $\Phi_m(X) = \Phi_{m_0/2}(X^{2m/m_0})$. Hence in any cases $\Phi_m(X)$ has the same number of coefficients than $\Phi_{m'}(X)$, where $m' = \prod_{\substack{i=2\\ e_i\neq 0}}^{r} p_i$.

Suppose that $r \geq 3$ then there exists $j \geq 3$ such that $m' = p_j\mu$ and $\gcd(p_j, \mu) = 1$ (in other words m' is divisible by a prime other than 3). A well known result on cyclotomic polynomials states that $\Phi_{p_j\mu}(X) = \frac{\Phi_\mu(X^{p_j})}{\Phi_\mu(X)}$.

Let $\Phi_\mu(X) = X^t + a_sX^s + \cdots + 1$, $(t > 0)$, then $\frac{\Phi_\mu(X^{p_j})}{\Phi_\mu(X)} = X^{(p_j-1)t} - a_sX^{(p_j-2)t+s} + \cdots = \Phi_{m'}(X)$. If $\Phi_{m'}(X)$ has only two coefficients then $(p_j - 2)t = -s$, since $t > 0$. It implies $p_j = 2$ which is impossible since $j \geq 3$.

If $\Phi_{m'}(X)$ has only three coefficients, due to (b), it implies that $(p_j-2)t+s = (p_j-1)t/2$, which gives $2s = (3-p_j)t$. Now, $2s \geq 0$ and $(3-p_j)t < 0$ since $p_j \geq 5$. Hence $r \leq 2$ and so $m = 2^{e_1}3^{e_2}$. From the definition of cyclotomic polynomials, we deduce that if $\Phi_m(X)$ has two coefficients the $m = 2^{e_1}$ with $e_1 \geq 1$, and when $\Phi_m(X)$ has three coefficients then $m = 2^{e_1}3^{e_2}$ with $e_1 \geq 0$ and $e_2 \geq 1$.

Hence, suitable cyclotomic polynomials are :

- $\Phi_{2^i}(X) = X^{2^{i-1}} + 1$, thus $n = 2^{i-1}$ with $i \geq 2$,
- $\Phi_{3^j}(X) = X^{2.3^{j-1}} + X^{3^{j-1}} + 1$, thus $n = 2.3^{j-1}$ with $j \in \mathbb{N}^*$,
- $\Phi_{2^i.3^j}(X) = X^{2^i.3^{j-1}} - X^{2^{i-1}.3^{j-1}} + 1$, thus $n = 2^i.3^{j-1}$ for $i, j \in \mathbb{N}^*$.

Conversely, it is clear that the above polynomials are by construction suitable cyclotomic polynomials. □

3.4. Suitable PMNS reduction $\{-1,1\}$-quadrinomials

In [9], Finch and Jones give criteria of irreducibility for polynomials $X^a + \beta X^b + \gamma X^c + \delta$ with $\beta, \gamma, \delta \in \{-1,1\}$ and $a > b > c > 0$. They suppose that $\gcd(a,b,c) = 2^t m$ with m odd and they note $a' = a/2^t$, $b' = b/2^t$ and $c' = c/2^t$. They define $\overline{a} = \gcd(a', b'-c')$, $\overline{b} = \gcd(b', a'-c')$ and $\overline{c} = \gcd(c', a'-b')$.

Proposition 3.4 (Theorem 2 in [9]). *The quadrinomial $X^a + \beta X^b + \gamma X^c + \delta$ is irreducible over $\mathbb{Z}[X]$, if and only if, its satisfies one of the following conditions :*

1. $(\beta,\gamma,\delta) = (1,1,1)$ *and* $\overline{a}\overline{b}\overline{c} \equiv 1 \pmod 2$
2. $(\beta,\gamma,\delta) = (-1,1,1)$, $b'-c' \not\equiv 0 \pmod{2\overline{a}}$, $b' \not\equiv 0 \pmod{2\overline{b}}$ *and* $a'-b' \not\equiv 0 \pmod{2\overline{c}}$
3. $(\beta,\gamma,\delta) = (1,-1,1)$, $b'-c' \not\equiv 0 \pmod{2\overline{a}}$, $a'-c' \not\equiv 0 \pmod{2\overline{b}}$ *and* $c' \not\equiv 0 \pmod{2\overline{c}}$
4. $(\beta,\gamma,\delta) = (1,1,-1)$, $a' \not\equiv 0 \pmod{2\overline{a}}$, $b' \not\equiv 0 \pmod{2\overline{b}}$ *and* $c' \not\equiv 0 \pmod{2\overline{c}}$
5. $(\beta,\gamma,\delta) = (-1,-1,-1)$, $a' \not\equiv 0 \pmod{2\overline{a}}$, $a'-c' \not\equiv 0 \pmod{2\overline{b}}$ *and* $a'-b' \not\equiv 0 \pmod{2\overline{c}}$

We call this class of suitable reduction quadrinomials `ClassQuadrinomials`*, and* `ClassQuadrinomials(n)` *is the set of such quadrinomials of degree n.*

For example, $E(X) = X^{2^t 7m} + X^{2^t 5m} + X^{2^t 3m} + 1$ is a suitable PMNS reduction quadrinomial.

3.5. Suitable PMNS reduction $\{-1,1\}$trinomials

In this part we refer to a paper of W.H. Mills [17] and one of W. Ljunggren [14]. The first one given criterion on quadrinomials and roots of unity, the second one given an application to trinomials.

Proposition 3.5. *We note* $\gcd(n,m) = d$ *and* $n = d.n_1$*,* $m = d.m_1$*. If* $n_1+m_1 \not\equiv 0 \mod 3$ *then the polynomial* $X^n + \beta X^m + \delta$ *with* $\delta, \beta \in \{-1, 1\}$ *and* $n > 2m > 0$ *is irreducible over* $\mathbb{Z}[X]$*.*

The class of the suitable reduction trinomials verifying these criteria is named `ClassTrinomials`*, and* `ClassTrinomials(n)` *represents the set of the trinomials of degree n.*

Proof. Let us transform, like in [14], $E(X) = X^n + \beta X^m + \delta$ in quadrinomial :

$$(X^n + \beta X^m + \delta)(X^n - \delta) = X^{2n} + \beta X^{n+m} - \beta\delta X^m - 1 = F(X).$$

Theorem 2 of [17], states that if $F(X) = A(X)E(X)$ where every root of $A(X)$ and no roots of $E(X)$ is root of unity then $E(X)$ is irreducible except if there exists r such that :

— $(2n, n+m, m) = (8r, 7r, r)$ and $(\beta, \delta) = (1, -1)$ or $(-1, -1)$,

— or, $(2n, n+m, m) = (8r, 4r, 2r)$ and $(\beta, \delta) = (1, -1)$,

— or, $(2n, n+m, m) = (8r, 6r, 4r)$ and $(\beta, \delta) = (-1, -1)$

It is easy to check that there is no integer r which satifies any of these 3 constraints, hence we only have to verify that no roots of $E(X)$ is a root of unity. First notice that, because $n = dn_1$ and $m = dm_1$ with $\gcd(n_1, m_1) = 1$, if λ is a root of $E(X)$ then λ^d is root of $X^{n_1} + \beta X^{m_1} + \delta$. Hence, if the roots of $X^{n_1} + \beta X^{m_1} + \delta$ are not roots of unity, then no root of $E(X) = X^n + \beta X^m + \delta$ is a root of unity.

Let us assume that λ is a root of $X^{n_1} + \beta X^{m_1} + \delta$, which is also a root of unity, then there exits $t > 1$ and k with $\gcd(k, t) = 1$, such that :

$$\lambda = e^{\frac{2ik\pi}{t}} = \cos\frac{2k\pi}{t} + i\sin\frac{2k\pi}{t}$$

Assume that $\beta = 1$, then

$$\begin{cases} \cos(\frac{2n_1k\pi}{t}) + \cos(\frac{2m_1k\pi}{t}) = 2\cos(\frac{k\pi(n_1+m_1)}{t})\cos(\frac{k\pi(n_1-m_1)}{t}) = -\delta \\ \sin(\frac{2n_1k\pi}{t}) + \sin(\frac{2m_1k\pi}{t}) = 2\sin(\frac{k\pi(n_1+m_1)}{t})\cos(\frac{k\pi(n_1-m_1)}{t}) = 0 \end{cases}$$

Last equality implies that $\sin(\frac{k\pi(n_1+m_1)}{t}) = 0$ or $\cos(\frac{k\pi(n_1-m_1)}{t}) = 0$. Since $\delta \neq 0$, first equation implies that $\cos(\frac{k\pi(n_1-m_1)}{t}) \neq 0$, hence $\frac{k(n_1+m_1)}{t}$ is an integer. Since $\gcd(k, t) = 1$, $t \mid (n_1 + m_1)$. This last result implies that first equation can be reduced to

$$\cos\left(\frac{k\pi(n_1 - m_1)}{t}\right) = \pm\frac{1}{2}$$

because $\delta = \pm 1$.

It means that

$$\frac{k\pi(n_1-m_1)}{t} = j\frac{\pi}{3}, \quad j = 1,2,4,5 \pmod 6)$$

Hence, $t \mid 3(n_1 - m_1)$, since $\gcd(k,t) = 1$

Assume that $\beta = -1$, the system becomes :

$$\begin{cases} \cos(\frac{2n_1k\pi}{t}) - \cos(\frac{2m_1k\pi}{t}) = -2\sin(\frac{k\pi(n_1+m_1)}{t})\sin(\frac{k\pi(n_1-m_1)}{t}) = -\delta \\ \sin(\frac{2n_1k\pi}{t}) - \sin(\frac{2m_1k\pi}{t}) = 2\cos(\frac{k\pi(n_1+m_1)}{t})\sin(\frac{k\pi(n_1-m_1)}{t}) = 0 \end{cases}$$

First equation implies that $\sin(\frac{k\pi(n_1-m_1)}{t}) \neq 0$, hence the second equation gives $\frac{k\pi(n_1+m_1)}{t} = j\frac{\pi}{2}$ for j odd, which implies $t \mid 2(n_1 + m_1)$. Since $\frac{k\pi(n_1+m_1)}{t} = j\frac{\pi}{2}$ for j odd, then first equation can be reduced to $\sin(\frac{k\pi(n_1-m_1)}{t}) = \pm\frac{1}{2}$, which means that

$$\frac{k\pi(n_1-m_1)}{t} = j\frac{\pi}{6}, \quad j = 1,5,7,11 \pmod{12}.$$

Hence $t \mid 6(n_1 - m_1)$.

To sum up if λ is a t^{th} root of unity of $X^{n_1} + \beta X^{m_1} + \delta$ with $\delta, \beta \in \{-1, 1\}$ then :

(a) if $\beta = 1$, $t \mid (n_1 + m_1)$ and $t \mid 3(n_1 - m_1)$

(b) if $\beta = -1$, $t \mid 2(n_1 + m_1)$ and $t \mid 6(n_1 - m_1)$

The case (a) implies that if $3 \nmid t$ then $t \mid (n_1 - m_1)$, thus $t \mid 2n_1$ and $t \mid 2m_1$, as $\gcd(n_1, m_1) = 1$ then $t = 2$ and $\lambda = 1$ or -1 is a root of $E(X)$ which is impossible.

The case (b) implies that if $3 \nmid t$, then $t \mid 2(n_1 - m_1)$, thus $t = 4$ then $\lambda = i$, $-i$, 1 or -1 is a root of $E(X)$ which is impossible.

Hence, if one root of $E(X)$ is a root of unity then 3 divides t, and then $n_1 + m_1 \equiv 0 \mod 3$.

Conclusion, if $\gcd(n_1, m_1) = 1$ and $n_1 + m_1 \not\equiv 0 \mod 3$ then $X^{n_1} + \beta X^{m_1} + \delta$ and $X^n + \beta X^m + \delta$ are irreducible.

□

3.6. Cases of irreducibility of binomials $X^n + c$, $c \in \mathbb{Z}$, $|c| \geq 2$, over $\mathbb{Z}$

Proposition 3.6. *We note, $c = \prod_{j=1}^{k} p_j^{m_j}$ with p_j pair-wise distinct prime numbers, and m_j positive integers. If $\gcd(m_1, \ldots, m_k, n) = 1$ then the polynomial $X^n + c$ with $c \in \mathbb{Z}$, $|c| \geq 2$, is irreducible over $\mathbb{Z}[X]$.*

We call this class of suitable polynomials `ClassBinomial`, *and, for n and c satisfying this proposition,* `ClassBinomial(n, c)` *is the singleton $\{X^n + c\}$.*

Proof. It is a direct application of the Corollary 1.2 of a paper due to Nicolae Ciprian Bonciocat [6].

□

3.7. Polynomials with bounds on the modules of their complex roots

The two propositions given in this part are inspired by the Perron irreducibility criterium, which is proved thanks to Rouché's theorem [5].

Proposition 3.7. *For a fixed $n \geq 2$, a prime μ, and $P(X) = X^n + \sum_{i=1}^{n/2} \varepsilon_i X^i \pm \mu$ with $\varepsilon_i \in \{-1, 0, 1\}$, if $\mu > 1 + \sum_{i=1}^{n/2} |\varepsilon_i|$ then the polynomial $P(X)$ is irreducible over $\mathbb{Z}[X]$.*

They represent the fifth class of suitable reduction polynomials. We call this class `ClassPrimeCst`*, and* $\mathtt{ClassPrimeCst}(\mathtt{n}, \mu)$ *represents all the polynomials of this class with $n \geq 2$ and μ a prime number .*

Remark. If $\mu > n/2 + 1$, then $\mathtt{ClassPrimeCst}(\mathtt{n}, \mu)$ contains $3^{n/2}$ elements (for each ε_i three possibilities), else $\sum_{i=0}^{\mu-2} \left(\begin{array}{c} n/2 \\ i \end{array} \right) 2^{i+1}$ elements.

Proof. Since $\mu > 1 + \sum_{i=1}^{n/2} |\varepsilon_i|$, then there exists $\delta > 1$ such that $\mu > \delta^n \left(1 + \sum_{i=1}^{n/2} |\varepsilon_i| \right)$.

Let us consider $\mathcal{C} = \{z \in \mathbb{C} \ / \ |z| = \delta\}$, $P(X) = X^n + \sum_{i=1}^{n/2} \varepsilon_i X^i + \varepsilon\mu$ ($\varepsilon_i \in \{-1, 0, 1\}$, $\varepsilon \in \{-1, 1\}$,), $F(X) = \varepsilon\mu$ and $G(X) = P(X) - F(X)$.

On $\mathcal{C}$ we have, $|G(z)| \leq \delta^n \left(1 + \sum_{i=1}^{n/2} |\varepsilon_i| \right) < \mu = |F(z)|$.

Since $F(z)$ and $G(z)$ are holomorphic functions, Rouché's theorem states that $F(z)$ and $P(z) = F(z) + G(z)$ have the same number of roots inside $\mathcal{C}$. Hence $P(z)$ has no root inside $\mathcal{C}$ since $F(z)$ is constant. In other words, any root α of $P(z)$ satisfies $|\alpha| \geq \delta > 1$.

Assume now, that $P(X)$ is reducible over $\mathbb{Z}[X]$. Hence, $P(X) = H(X)Q(X)$ with $H(X)$ and $Q(X)$ two monic polynomials. Since $|P(0)| = \mu$ (a prime number), we can assume that $|H(0)| = \mu$ and $|Q(0)| = 1$. Now $\prod |z_i| = 1$, where z_i are all the roots of $Q(X)$. But the roots of $Q(X)$ are also roots of $P(X)$ which is not possible since any root α of $P(X)$ is such that $|\alpha| \geq \delta > 1$.

Hence, $P(X)$ is irreducible over $\mathbb{Z}[X]$.

□

Proposition 3.8. *For a fixed $n \geq 2$, and $P(X) = X^n + \sum_{i=2}^{n/2} \varepsilon_i X^i + a_1 X \pm 1$ with*

$\varepsilon_i \in \{-1,0,1\}$ and $a_1 \in \mathbb{Z}^*$. If $|a_1| > 2 + \sum\limits_{i=2}^{n/2} |\varepsilon_i|$ then the polynomial $P(X)$ is irreducible over $\mathbb{Z}[X]$.

We call this class `ClassPerron`*, and* $\texttt{ClassPerron}(\texttt{n}, \texttt{a}_1)$ *represents all the polynomials of this class with $n \geq 2$, $a_1 \in \mathbb{Z}^*$.*

Remark. If $|a_1| > n/2+1$, then $\texttt{ClassPerron}(\texttt{n}, \texttt{a}_1)$ contains $2 \times 3^{n/2-1}$ elements, else $\sum\limits_{i=0}^{|a_1|-3} \begin{pmatrix} n/2-1 \\ i \end{pmatrix} 2^{i+1}$ elements.

Proof. The proof is similar to the previous one. From $|a_1| > 2 + \sum_{i=2}^{n/2} |\varepsilon_i|$, we can deduce that there exists $\delta > 1$ such that $|a_1| > \delta^n \left(2 + \sum_{i=2}^{n/2} |\varepsilon_i|\right)$. Then, from Rouché's theorem, $P(z)$ and $F(z) = a_1 z$ have the same number of roots inside $\mathcal{C} = \{z \in \mathbb{C} \ / \ |z| = \delta\}$. Hence $P(z)$ has only one root whose module is strictly less than δ.

Now is $P(X)$ is reducible over $\mathbb{Z}[X]$, then $P(X) = H(X)Q(X)$, with $H(X)$ and $Q(X)$ two monic polynomials and $|H(0)| = |G(0)| = 1$. Hence $H(z)$ has at least one root z_H such that $|z_H| \leq 1$ and $G(z)$ has at least one root z_G such that $|z_G| \leq 1$. It means that $P(z)$ has at least two roots inside $\mathcal{C}$, which is not possible.

Hence, $P(X)$ is irreducible over $\mathbb{Z}[X]$.

□

4. Number of PMNS from the roots of their reduction polynomial modulo p

In this section, we determine for each class, the reduction polynomials which have one or more roots γ in $\mathbb{Z}/p\mathbb{Z}$. The number of its roots in $\mathbb{Z}/p\mathbb{Z}$ defines the number of possible PMNS.

As we need to present several compact PMNS with an efficient arithmetic on representations from a prime p and a number of digits n, finding relevant reduction polynomials is crucial. Now that we have described classes of irreducible polynomials with specific reduction properties, we need to identify for a prime p which ones have at least one root in $\mathbb{Z}/p\mathbb{Z}$, and if possible, how many. We begin with a presentation of two special cases where the reduction polynomials are cyclotomics or binomials, then we propose a method in the general case, that works for any irreducible integer polynomials.

4.1. Number of PMNS with a cyclotomic reduction polynomial

Proposition 4.1. *Let $p > 2$ a prime number, and an integer $m \geq 3$ such that $m \mid (p-1)$ then the cyclotomic polynomial $\Phi_m(X) \mid (X^{p-1} - 1)$ and $\Phi_m(X)$ has $\varphi(m)$ roots over $\mathbb{Z}/p\mathbb{Z}$.*

Proof. We have, $(X^{p-1}-1) = \prod_{\xi_i \in (\mathbb{Z}/p\mathbb{Z})^*} (X-\xi_i) = \prod_{d|(p-1)} \Phi_d(X)$.

Thus $\Phi_m(X) \mid \prod_{\xi_i \in (\mathbb{Z}/p\mathbb{Z})^*} (X-\xi_i)$, and $\Phi_m(X)$ has $\varphi(m)$ (its degree) roots over $\mathbb{Z}/p\mathbb{Z}$ □

We apply Proposition 4.1 to the different cyclotomic polynomial of the class `ClassCyclo(n)` introduced in Proposition 3.3.

Corollary 4.1. *Let p prime, $n \geq 2$ such that $n = 2^i 3^j$, with $i, j \in \mathbb{N}$.*

- *If $i > 0$, $j = 0$, and $(2\,n)$ divides $(p-1)$, and $E(X) = \Phi_{2n}(X) = X^n + 1$,*
- *If $i = 1$, $j \geq 0$, and $(3\,n\,/\,2)$ divides $(p-1)$, and $E(X) = \Phi_{\frac{3n}{2}}(X) = X^n + X^{\frac{n}{2}} + 1$,*
- *If $i \geq 1$, $j \geq 0$, and $(3\,n)$ divides $(p-1)$, and $E(X) = \Phi_{3n}(X) = X^n - X^{\frac{n}{2}} + 1$,*

then, there exist n PMNS $(p, n, \gamma_i, \rho)_{E(X)}$, with γ_i one of the n distinct roots modulo p of $E(X)$.

Example 4.1. Construction PMNS from a cyclotomic reduction polynomial for $p = 2^{256}.3^{157}.115 + 1$ coded on 512 bits.

— $E(X) = X^8 + 1$, from the height roots, the best ρ is obtained with Corollary 2.1 and Corollary 2.2., and is 66 bits long.

— $E(X) = X^6 + X^3 + 1$, from the six roots, the best ρ is obtained two times with LLL, else with Corollary 2.1 and Corollary 2.2, and is 87 bits long.

— $E(X) = X^6 - X^3 + 1$, from the six roots, the best ρ is obtained with Corollary 2.1 and Corollary 2.2, and is 87 bits long.

4.2. Number of PMNS with reduction binomials $X^n + c$, $c \in \mathbb{Z}$, $|c| \geq 2$

Proposition 4.2. *Let $E(X) = X^n + c$ an element of* `ClassBinomial(n, c)` *(Proposition 3.6). Let g a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and y such that $g^y \equiv -c \mod p$.*

If $\gcd(n, p-1)$ divides y, then, $E(X) = X^n + c$ has $\gcd(n, p-1)$ different roots.

Remark. If $\gcd(n, p-1) = 1$ then $E(X) = X^n + c$ is guanrantee to have one root.

Proof. Let X_0 a solution of $E(X) = 0 \pmod{p}$. Then there exists x_0 such that, $X_0 \equiv g^{x_0} \pmod{p}$ and $g^{n.x_0} \equiv -c \equiv g^y \pmod{p}$. In other words, $n.x_0 \equiv y \pmod{p-1}$.

Now, let $\delta = \gcd(n, p-1)$, a classical result in modular arithmetic states that this linear equation admits δ solutions iff δ divides y, each solution being equal to $x_0 + jp'$ where $j \in \{0, \ldots, \delta - 1\}$ and $(p-1) = \delta p'$.

□

Example 4.2. For $p = 40993$, 5 is a generator of $(\mathbb{Z}/40993\mathbb{Z})^*$ Let $n = 4$ and $E(X) = X^4 + c$. For $c = 2$, we can find $y = 33788$, such that $-c = 5^y \mod p$. Since $\gcd(1, n) = 1$, from Prop 4.2 $E(X)$ is irreducible. Morerover, $\gcd(n, p-1) = 4$ divides y, hence four PMNS can be generated from $E(X)$. For $c' = -2$, we can find $y' = 13292$ and $\gcd(n, p-1) = 4$ divides y' giving once again four possible PMNS.

4.3. Number of PMNS in the general case

In this part, we propose a general method to count the minimum number of PMNS we can reach from a prime p and any irreducible polynomial in $\mathbb{Z}[X]$.

We use the fact that the computation of $\gcd(X^p - X, E(X)) \mod p$ can be done, in a reasonable time, in two steps :

1. we compute $X^p \bmod E(X) \bmod p$ with a square and multiply exponentiation algorithm, and we compute $F(X) = X^p - X \bmod E(X) \bmod p$,
2. then, we evaluate $\gcd(F(X), E(X)) \bmod p$ with polynomials of degrees lower or equal to n.

The first step represents at most $\log(p)$ squares and multiplications, and the second step represents at most n iterations of the Euclidean algorithm. The roots are found by factorising the polynomial $\gcd(F(X), E(X)) \bmod p$. Some examples of factorization algorithms can be found in [19].

Proposition 4.3. *Let p prime, $n > 2$, $E(X)$ a polynomial of degree n and irreducible in $\mathbb{Z}[X]$, and $D(X) = \gcd(X^p - X, E(X)) \mod p$, there exists* $\deg(D(X))$ *Polynomial Modular Number Systems* $(p, n, \gamma_i, \rho)_{E(X)}$.

Proof. The proof is trivial considering, when p is prime, that the roots of $X^p - X \mod p$ are the p elements of $\mathbb{Z}/p\mathbb{Z}$. □

Remark. Proposition 4.1 can be considered as a corollary of this Proposition 4.3.

Example 4.3. We consider $p = 78264746924694600393874000999999297$ and $E(X) = X^5 + X^2 + 1$.

Then, $X^p \bmod E(X) =$ $73221262594200981770939850990946624\ X^4$
$+17278262153012433490422224611352 62\ X^3$

$$\begin{aligned}
\text{Then, } X^p \bmod E(X) = \;& 7322126259420098177093985099094624\ X^4\\
&+1727826215301243349042222461135262\ X^3\\
&+3438841897608126971004523506864410\ X^2\\
&+7372958503626664659096728485020295\ X\\
&+4167285606168530025180293516680876
\end{aligned}$$

$$\begin{aligned}
\text{Thus, } \;& \gcd(X^p \bmod E(X) - X, E(X)) \bmod p\\
&= X^2 + 1305849998419067291000337897705258\ X\\
&+1793073000954204546034194068098826\\
&= (X + 6157699039557809270671068895070912)\\
&(X + 2974625651330718059716669102633643)
\end{aligned}$$

Hence, we obtain two roots of $E(X) \bmod p$:

$$\gamma_1 = 16687756529116507687163312049 28385$$

$$\gamma_2 = 48518490411387419796707309973 65654$$

4.4. *Example giving all the possible PMNS for a given p*

This example is obtained with SageMath subroutines.

For $p = 57896044618658097711785492504343953926634992332820282019728792003956566811073$ a 256-bits prime, and $n = 9$.

We consider PMNS $\mathfrak{B} = (p, n, \gamma, \rho)_E$ such that :

— $E(X) = X^n + a_k X^k + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, with $n \geq 2$ and $k \leq \frac{n}{2}$,

— coefficients $|a_i| \leq 1$ for $1 \leq i \leq k$ and $|a_0| \leq 3$

— $\rho \leq 2^{31}$

The number of PMNS $\mathfrak{B} = (p, n, \gamma, \rho)_E$ that can be built for different polynomials verifying the criteria is equal to 354.

Most of the time, the best ρ is obtained first by LLL (266 times) or BKZ (46), some are due to Corollary 2.1 (10) or with Corollary 2.2 (28), or Proposition 2.3 (4) with a short vector.

5. Conclusion

In this paper, we have shown with Theorem 2.1, the link between the existence of a PMNS and the Euclidean lattice generated by its reduction polynomial and its modulo. We thus have a bound on the size of the digits corresponding to the covering radius. Then, Theorem 2.2 gives us a bound which can be easily calculate from the norm 1 of the lattice. This second theorem has led us to consider PMNS defined by an irreducible polynomial. In this case, it is easy to define a base of the lattice that can be associated to the PMNS (Proposition 2.3, Corollaries 2.1 and 2.2). These theorems, propositions and corollaries allowed us to produce PMNS with specific reduction polynomials allowing efficient reductions and whose roots give the radices of these systems. Now, we have the opportunity to offer for a given modulo p a wide variety of PMNS.

Acknowledgement

This work was partially supported by the ANR project ARRAND 15-CE39-0002-01.

Références

[1] L. Babai. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1) :1–13, 1986.

[2] J.C. Bajard, L. Imbert, and T. Plantard. Arithmetic operations in the polynomial modular number system. In *17th IEEE Symposium on Computer Arithmetic (ARITH'05)*, pages 206–213. IEEE, 2005.

[3] J.C. Bajard, L. Imbert, and T. Plantard. Modular number systems : Beyond the Mersenne family. In *Selected Areas in Cryptography*, pages 159–169. Springer, 2005.

[4] P.D. Barrett. Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor. In Springer-Verlag, editor, *Advances in Cryptology, Proc. Crypto'86*, volume 263 of *LNCS*, pages 311–323, 1987.

[5] N. C. Bonciocat. On an irreducibility criterion of Perron for multivariate polynomials. *Bull. Math. Soc. Sci. Math. Roumanie*, 53(101)(3) :213–217, 2010.

[6] N. C. Bonciocat. Schönemann–Eisenstein–Dumas-type irreducibility conditions that use arbitrarily many prime numbers. *Journal Communications in Algebra*, 43(8), 2015.

[7] L.-S. Didier, F.-Y. Dosso, N. El Mrabet, J. Marrez, and P. Véron. Randomization of Arithmetic over Polynomial Modular Number System. In *26th IEEE International Symposium on Computer Arithmetic*, Kyoto, Japan, June 2019. to appear.

[8] G. Dumas. Sur quelques cas d'irreductibilité des polynômes à coefficients rationnels. *Journal de Mathématique Pure et Appliquée*, 2, 1906.

[9] C. Finch and L. Jones. On the irreducibility of -1,0,1-quadrinomials. *INTEGERS : Electronic Journal of Combinatorial Number Theory*, 6, 2006.

[10] S.D. Galbraith. *Mathematics of Public Key Cryptography.* Cambridge University Press, 2012.

[11] G. Hanrot, X. Pujol, and D. Stehlé. Algorithms for the shortest and closest lattice vector problems. In *International Conference on Coding and Cryptology*, pages 159–190. Springer, 2011.

[12] D. Harvey and J. van der Hoeven. Faster integer multiplication using short lattice vectors. In msp, editor, *Thirteenth Algorithmic Number Theory Symposium ANTS XIII*, 2019.

[13] T. Laarhoven, J. van de Pol, and B. de Weger. Solving hard lattice problems and the security of lattice-based cryptosystems. Cryptology ePrint Archive, Report 2012/533, 2012.

[14] W. Ljunggren. On the irreducibility of certain trinomials and quadrinomials. *Mathematica Scandinavica*, volume 8(n^o 1) :65–70, 1960.

[15] A. Menezes, S. A. Vanstone, and P. C. van Oorschot. *Handbook of Applied Cryptography.* CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1996.

[16] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems : a cryptographic perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science.* Kluwer Academic Publishers, 2002.

[17] W. H. Mills. The factorization of certain quadrinomials. *Mathematica Scandinavica*, 57, 1985.

[18] P.L. Montgomery. Modular multiplication without trial division. *Mathematics of Computation*, 44 :519–521, 1985.

[19] P. Naudin and C. Quitté. Univariate polynomial factorization over finite fields. *Theoretical Computer Science*, 191(1-2) :1–36, January 1998.

[20] T. Plantard. *Arithmétique modulaire pour la cryptographie.* Theses, Université Montpellier II - Sciences et Techniques du Languedoc, 2005.

[21] T. Plantard, W. Susilo, and Z. Zhang. LLL for ideal lattices : re-evaluation of the security of gentry–halevi's fhe scheme. *Designs, Codes and Cryptography*, volume 76(n^o 2) :325–344, 2015.

[22] J. A. Solinas. Generalized Mersenne numbers. Technical Report CORR-99-39, Center for Applied Cryptographic Research, University of Waterloo., 1999.